CMS Manual System	**Department of Health & Human Services (DHHS)**
Pub 100-17 Medicare Business Partners Systems Security	**Centers for Medicare & Medicaid Services (CMS)**
Transmittal 11570	**Date: August 19, 2022**
	Change Request 12652

SUBJECT: Pub 100-17 Medicare Business Partners Systems Security Manual Update

I. SUMMARY OF CHANGES: The Information Security and Privacy Group (ISPG) has provided updated security requirements, the Acceptable Risk Safeguards (ARS) version 5.0 (previously version 3.1). As a result, the CMS Medicare Contractor Management Group (MCMG) has updated IOM 100-17 which contains the Business Partner System Security Manual (BPPSM) and the Medicare Administrative Contractor (MAC) ARS.

The purpose of this CR is to have the MACs perform an analysis regarding the attached BPSSM revision 15, which includes the updated MAC ARS security requirements, to evaluate cost and operational impacts, and to provide a level of effort to CMS detailing what is required to implement the updates. The MACs shall review the BPSSM and the MAC ARS controls entirely and carefully as there have been significant changes and additions. Additional documentaton has been attached to this CR (Full ARS 5.xlsx) which contains a CMS ARS Redline column to allow for comparison between ARS 5.0 and the previous version ARS 3.1.

As part of the process for implementing the updated security requirements, the MACs shall review the updated BPSSM and MAC ARS control set to evaluate the documented requirements to fully determine possible impacts. MACs shall consider the workload associated with the planning, implementation, education and ongoing support required to meet the security requirements in their analysis.

EFFECTIVE DATE: March 7, 2022
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: April 3, 2023 - Complete implementation of all controls associated with IOM 100-17 as described in this CR; March 7, 2022 - For MACs to provide their level of effort for implementing all of the controls associated with IOM 100-17 as described in this CR. MACs may begin work on this CR upon placement on their contract.

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated)
R=REVISED, N=NEW, D=DELETED-*Only One Per Row.*

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
N	IOM 100-17 contains the BPSSM. Within the BPSSM is the MAC ARS 5.0.

III. FUNDING:
For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined

in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

IV. ATTACHMENTS:

Business Requirements
Manual Instruction

Attachment - Business Requirements

Pub. 100-17	Transmittal: 11570	Date: August 19, 2022	Change Request: 12652

SUBJECT: Pub 100-17 Medicare Business Partners Systems Security Manual Update

EFFECTIVE DATE: March 7, 2022
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: April 3, 2023 - Complete implementation of all controls associated with IOM 100-17 as described in this CR; March 7, 2022 - For MACs to provide their level of effort for implementing all of the controls associated with IOM 100-17 as described in this CR. MACs may begin work on this CR upon placement on their contract.

I. GENERAL INFORMATION

A. Background: This is an update to the existing Business Partners Systems Security Manual (BPSSM) and the Medicare Administrative Contractor Acceptable Risk Safeguards (MAC ARS). The BPSSM provides clarification and support to various CMS security policies, standards guidelines and procedures. The MAC ARS is based on NIST Special Publication 800-53 Revision 5, dated September, 2020 and has been customized for usage by the MACs.

B. Policy: This CR is to ensure compliance with the Federal Information Security Management Act (FISMA) of 2014, National Institute of Standards and Technology (NIST) requirements and guidance, and CMS policies, standards, guidelines and procedures.

II. BUSINESS REQUIREMENTS TABLE

"Shall" denotes a mandatory requirement, and "should" denotes an optional requirement.

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
12652.1	Medicare Administrative Contractors (MACs) shall perform an analysis to determine level of effort to implement BPSSM version 15 and the associated MAC Acceptable Risk Safeguards (ARS). Relationships with any affected subcontractors should be considered/included in the analysis and the impacts to the subcontractor should be identifiable within the analysis.	X	X	X	X					
12652.1.1	MACs shall not request funding for any control that has been identified as fully inheritable. The attached Excel spreadsheet, Full ARS 5.xlsx, provides details in Column G - Responsibility. Any control having a Responsibility entry of only OCISO will not be funded.	X	X	X	X					

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
12652.1.2	Upon completion of the analysis of the proposed BPSSM and MAC ARS changes, MACs shall submit an estimate that details the level of effort ***by each specified control that requires funding*** broken down by planning, implementation and on-going support for implementing any required changes. Controls determined to not have any associated costs shall be excluded from this submission. The MACs shall evaluate all changes and submit only those changes that will result in cost and effort changes within their environment. This estimate should be delivered to Frank Schreibman, (Frank.Schreibman@cms.hhs.gov) and uploaded to the CR estimates portion of ECHIMP by March 7, 2022. Any submission that does not clearly indicate the control, actions necessary and level of effort for a specific change will be returned for updating. **NOTE:** CMS is expecting the MACs to submit their full and complete level of effort (LOE) estimates in ECHIMP related to the draft CR prior to its issuance.	X	X	X	X					
12652.2	Contractors shall be in compliance with any requirements updated in the Business Partner System Security Manual (BPSSM) and Medicare Administrative Contractor (MAC) Acceptable Risk Safeguards (ARS).	X	X	X	X					

III. PROVIDER EDUCATION TABLE

Number	Requirement	Responsibility				
		A/B MAC			DME MAC	CEDI
		A	B	HHH		
	None					

IV. SUPPORTING INFORMATION

Section A: Recommendations and supporting information associated with listed requirements: N/A

"Should" denotes a recommendation.

X-Ref Requirement Number	Recommendations or other supporting information:

Section B: All other recommendations and supporting information: N/A

V. CONTACTS

Pre-Implementation Contact(s): Kevin Potter, 443-641-7890 or Kevin.Potter@cms.hhs.gov , Gregg Sanders, 443-510-9197 or Gregg.Sanders@cms.hhs.gov , Frank Schreibman, 443-764-4547 or frank.schreibman@cms.hhs.gov

Post-Implementation Contact(s): Contact your Contracting Officer's Representative (COR).

VI. FUNDING

Section A: For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

ATTACHMENTS: 2

MEDICARE ADMINISTRATIVE CONTRACTOR ACCEPTABLE RISK SAFEGUARDS (MAC ARS)

ARS 5.0

INTRODUCTION

This MAC ARS version 5 has been customized by the Medicare Contractor Management Group (MCMG) for use by the MACs and their subcontractors. This document contains all controls that are mandatory for the MACs and their subcontractors to implement.

The Business Partner System Security Manual (BPSSM) should be examined and referenced as it supersedes the ARS requirements. In order to assure you are meeting your contractual requirements, you need to pay attention to the full content of the BPSSM. There are controls in the ARS whose requirements have been redefined by the BPSSM for MAC implementation (e.g., periodic requirements that differ from the ARS). The BPSSM also provides definitions for organizationally defined variables in the ARS.

It is possible that implementation of a single control mechanism can address multiple controls. If that is the case, then each of the affected controls impacted should be documented separately, with details of how the control mechanism addresses each of the controls.

A note about the layout of this document. The Implementation Standards within this document follow the Discussion section. It is imperative that you consider the Implementation Standards when addressing each control. The Discussion section provides additional information regarding the meaning of the control and/or guidance for implementing the control but is not intended as specific technical direction, more like clarifying information.

This MAC ARS represents the complete set of controls that need to be implemented by the MACs.

Please note: As of May, 2022, the following controls have been added/removed from the MAC ARS at the direction of ISPG.

- Added
  - IA-12(06) – ACCEPT EXTERNALLY-PROOFED IDENTITIES
- Removed
  - IA-12(04) – In-Person Validation and Verification
  - IA-12(05) – Address Confirmation
  - PM-07(01) – Offloading

Access Control

Control Number	Control Name	Priority	CMS Baseline
AC-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel and roles:
  1. CMS Enterprise-level access control policy that:
    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
  2. Procedures to facilitate the implementation of the access control policy and associated access controls;
(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the access control policy and procedures; and
(c) Review and update the current access control:
  1. Policy at least every three (3) years and following CMS-defined events (e.g. assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).; and
  2. Procedures at least every three (3) years and following CMS-defined events (e.g. assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.
CMS provides an enterprise level access control policy within the CMS IS2P2, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures.)

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

IA-1, PM-9, PM-24, PS-8, SI-12;	Code: 5 United States Code (U.S.C.) §552a(b), §552a(e)(9)-(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	CNSSI: 4009;
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-1, SM-3;

	HIPAA: 45 C.F.R. §164.308(a)(3)(i), 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(4)(i), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.308(a)(4)(ii)(C), 45 C.F.R. §164.312(a)(1), 45 C.F.R. §164.514(d)(1)-(5);
	NISTIR: 7874;
	NIST SP: 800-12, 800-30, 800-37 Rev. 2 Appendix B, 800-39, 800-100, 800-122;
	OMB Circular: A-130 7.g. and Appendix III;
	OMB Memo: M-06-16, M-17-12 Att. 4;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII:
Access Control policies and procedures form the foundation that allows privacy protections to be implemented for the identified uses of personally identifiable information (PII) and protected health information (PHI). Privacy requirements commonly use the terms “adequate security” and “confidentiality” when referring to access controls and other security safeguards for PII. Applied together, these terms signify the need to make risk-based decisions based on the magnitude of harm (to CMS, its Businesses/Systems, and individuals) when determining applicable restrictions for PII. For this overlay, refer to the definitions of “adequate security” in OMB Circular A-130, Appendix III, and “confidentiality” in NIST SP 800-37, Rev. 2, Appendix B. These definitions are consistent with Committee for National Security Systems Instruction (CNSSI) No. 4009.
Systems processing, storing, or transmitting PHI:
High & Moderate:
PHI.1 - Develop, disseminate, and review/update the access control policies and procedures that comply with the HIPAA Minimum Necessary Rule, which includes permitted or required uses and disclosures, to limit unnecessary or inappropriate access to PHI.
PHI.2 - Policies and procedures to comply with the regulatory requirements governing an individual’s right to access copies of their PHI, including electronic copies.;
Discussion for systems processing, storing, or transmitting PHI:
Access control policies must complying with the HIPAA Minimum Necessary Rule and permitted or required uses and disclosures, to limit unnecessary or inappropriate access to PHI.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
High & Moderate:
PRIV.1 - Monitor for changes to applicable privacy laws, regulations, and overarching policy that affect access control policies no less often than once every 365 days to ensure the CMS and Mission/Business/System access control policies remains effective.
PRIV.2 - Ensure access control policies support privacy to the greatest extent feasible throughout the system's life cycle.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
AC-02	**Account Management**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

(a) Define and document the type of accounts allowed and specifically prohibited for use within the system (e.g., individual, group, system, application, guest/anonymous, emergency, and temporary);
(b) Assigns account managers;
(c) Require defined prerequisites and criteria for group and role membership;
(d) Specify;
1. Authorized users of the system;
2. Group and role membership; and
3. Access authorizations (i.e., privileges) and other attributes (as required) for each account;

(e) Require approvals by defined personnel or roles (defined in applicable security and privacy plans) for requests to create accounts;
(f) Create, enable, modify, disable, and remove accounts in accordance with Acceptable Risk Safeguards (ARS) requirements and Risk Management Handbook (RMH) standards and procedures;
(g) Monitor the use of accounts;
(h) Notify account managers and defined personnel or roles (defined in applicable security/privacy plans) within:
   1. thirty (30) days when accounts are no longer required;
   2. thirty (30) days when users are terminated or transferred; and
   3. thirty (30) days when system usage or need-to-know changes for an individual;
(i) Authorizes access to the system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions/business functions;
(j) Review accounts for compliance with account management requirements at least every 365 days for all systems; and
(k) Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
(l) Align account management processes with personnel termination and transfer processes.

Discussion

Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.

Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts. Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.

Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training.

Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Implementation Standard

High, Moderate & Low:
Std.1 - Remove or disable default user accounts. Rename active default accounts.
Std.2 - Implement centralized control of user access administrator functions.
Std.3 - Regulate the access provided to contractors and define security requirements for contractors.
Std.4 - Automated account management results must be searchable by the CMS Cybersecurity Integration Center (CCIC):
   (a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
   (b) Account management information sources include systems, appliances, devices, services, and applications (including databases); and

(c) CCIC-directed account management information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.

Std.5 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Std.6 - Notify account managers within a Mission/Business/System-defined timeframe not to exceed 30 days when temporary accounts are no longer required or when system users are terminated or transferred or system usage or need-to-know/need-to-share changes.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37;
	Reference Policy
	Code: 5 U.S.C. §552a(b), I(9)-(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-3, AC-3.1.4, AC-3.1.5, AC-3.1.6, AC-4.1.1, AS-2. AS-3.8.1;
	HIPAA: 45 C.F.R. §164.308(a)(4)(i), 45 C.F.R. §164.308(a)(4)(ii)(C), 45 C.F.R. §164.308(a)(5)(ii)(C), 45 C.F.R.§164.312(a)(2)(i), 45 C.F.R. §164.502;
	NIST SP: 800-162, 800-178, 800-192;
	OMB Circular: A-130;
	OMB Memo: M-17-12 Att. 1, M-16-04, M-19-03;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a) Define and document the type of accounts allowed and specifically prohibited for use within the system (e.g., individual, group, system, application, guest/anonymous, emergency, and temporary);

(b) Assigns account managers;

(c) Require defined prerequisites and criteria for group and role membership;

(d) Specify;

1. Authorized users of the system;
2. Group and role membership; and
3. Access authorizations (i.e., privileges) and other attributes (as required) for each account;

(e) Require approvals by at least two appropriate organizational personnel (e.g., System Owner, Business owner, AO, Chief Information Security Officer, etc.), or designee, for requests to create system accounts;

(f) Create, enable, modify, disable, and remove accounts in accordance with Acceptable Risk Safeguards (ARS) requirements and Risk Management Handbook (RMH) standards and procedures;

(g) Monitor the use of accounts;

(h) Notify account managers and defined personnel or roles (defined in applicable security/privacy plans) within:

1. thirty (30) days when accounts are no longer required;
2. thirty (30) days when users are terminated or transferred; and
3. thirty (30) days when system usage or need-to-know changes for an individual, and;
4. Notify appropriate organization personnel within 12 hours when temporary accounts or privileged accounts are no longer required, users are terminated or transferred, and when user's need-to-know changes

(i) Authorizes access to the system based on:

1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions;

(j) Review accounts for compliance with account management requirements at least every 365 days for all systems; and

1. Review privileged accounts no less often that quarterly for compliance with account management requirements. Privileged account access is to be reauthorized for the HVA no less often than annually. User accounts are to be reviewed no less often than annually for compliance with account management requirements;

(k) Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

<table>
<tr><td>(l) Align account management processes with personnel termination and transfer processes.</td></tr>
<tr><td><b>HVA Discussion</b>
Examples of HVA account types include individual, system, guest, emergency, developer, temporary, and service. Identification of authorized HVA users and the specification of access privileges reflects the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. External system accounts are not included in the scope of this control. Organizations should address external system accounts through organizational policy.</td></tr>
<tr><td><b>HVA Implementation Standard</b>
Item e: require approvals by at least two appropriate organizational personnel (e.g., system owner, mission/business owner, Authorizing Official, Chief Information Security Officer [CISO], etc.) for requests to create system accounts;
Item h: notify appropriate organization personnel within 12 hours when temporary accounts or privileged accounts are no longer required, users are terminated or transferred, and upon user’s need-to-know changes;
Item j: review privileged accounts, at least quarterly, for compliance with account management requirements. Privileged account access should be re-authorized for the HVA at least annually. Review user accounts, at least, annually for compliance with account management requirements; and
Item m: prohibit creating and using guest, anonymous, and shared HVA accounts (including shared administrator and root accounts) for access to all information types processed by the system. NOTE: Anonymous is allowed for read-only, public-facing information websites.</td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>AC-02(01)</b></td><td><b>Control Name</b>
<b>Automated System Account Management</b></td><td colspan="2"><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="5"><b>Control Statement</b>
Support the management of system accounts using automated mechanisms.</td></tr>
<tr><td colspan="5"><b>Discussion</b>
Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage. Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.</td></tr>
<tr><td colspan="5"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="3"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
None;</td><td colspan="3"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
FISCAM: AC-3.1.4, AC-3.1.5, AC-3.1.6, AC-4.1.1, AS-3.8.1;
OMB Memo: M-16-04, M-19-03;</td></tr>
<tr><td colspan="5"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="5"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="5"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="5"><b>HVA Discussion</b></td></tr>
<tr><td colspan="5"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
AC-02(02)</td><td><b>Control Name</b>
Automated Temporary and Emergency Account Management</td><td><b>Priority</b>
P1</td><td><b>CMS Baseline</b>
Moderate
High
HVA</td></tr>
<tr><td colspan="4"><b>Control Statement</b></td></tr>
</table>

Automatically disable emergency accounts within 24 hours of issuance (activation) and temporary accounts within a fixed duration not to exceed 30 days for High systems and 60 days for Moderate systems.

Discussion
Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

Implementation Standard
High & Moderate:
Std.1 - Emergency accounts will be automatically disabled within 24 hours of activation;
Std.2 - The duration of temporary accounts will not exceed:
(a) 30 days for High systems and
(b) 60 days for Moderate systems.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
None;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	OMB Memo: M-16-04, M-19-03;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement
Automatically disable temporary and emergency accounts within 12 hours of issuance (activation)within a fixed duration not to exceed 30 days for High systems and 60 days for Moderate systems.
This reduces the risk that Temporary and Emergency accounts, which typically do not have multi-factor authentication, are not a source of compromise

HVA Discussion
Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time-period, rather than at the convenience of the systems administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

HVA Implementation Standard
Automatically disable temporary and emergency accounts within 12 hours of issuance

Control Number	Control Name	Priority	CMS Baseline
AC-02(03)	**Disable Accounts**	**P1**	**Moderate** **High**

Control Statement
(a) Disable accounts within thirty (30) days when the accounts:
(1) Have expired;
(2) Are no longer associated with a user or individual;
(3) Are in violation of organizational policy; or
(b) Disable accounts when the accounts have been inactive within 30 days for High Systems or 60 days for Moderate Systems.
.

Discussion
Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

Implementation Standard
High & Moderate
Std.1 - Accounts will be disabled within 30 days when the accounts:
(a) Have expired;
(b) Are no longer associated with a user or individual;

(c) Are in violation of organizational policy; Std.2 - Accounts will be disabled when these accounts have been inactive: (a) Within 30 days for High systems or; (b) Within 60 days for Moderate systems.	
Control Review Frequency Two (2) Months	**Assessment Frequency** Annually (365 Days)

Related Controls
None;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	OMB Memo: M-16-04, M-19-03;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number AC-02(04)	**Control Name** Automated Audit Actions	**Priority** P1	**CMS Baseline** Moderate High
Control Statement Automatically audit account creation, modification, enabling, disabling, and removal actions.			
Discussion Account management audit records are defined in accordance with AU-2 and reviewed, analyzed, and reported in accordance with AU-6. Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.			
Implementation Standard High & Moderate: Std.1 - Automated account management audit action results are made available to the CCIC: (a) Information must be searchable by the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; and (b) Account management audit information sources include systems, appliances, devices, services, and applications (including databases). Std.2 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
AU-2, AU-6
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		OMB Memo: M-16-04, M-19-03;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-02(05)**	**Control Name** **Inactivity Logout**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement Require that users log out when the time-period of inactivity exceeds 90 minutes and at the end of the user’s normal work period.	
Discussion Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.	
Implementation Standard	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-11
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	OMB Memo: M-16-04, M-19-03;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
AC-02(07)	**Privileged User Accounts**		**Above Baseline**

Control Statement (a) Establish and administer privileged user accounts in accordance with a role based access scheme; (b) Monitor privileged role assignments; (c) Monitor changes to roles; and (d) Revoke access when privileged roles are no longer appropriate.	
Discussion	
Implementation Standard	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls	**Reference Policy**
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
AC-02(09)	**Restrictions on Use of Shared and Groups Accounts**	**P3**	**Above Baseline**

Control Statement Only permit the use of shared and group accounts when a business need can be documented and approved, in advance, by the Authorizing Official (AO). (a) When shared and/or group accounts are used, the applicable security and privacy plans must: 1. Describe how the shared and/or group accounts are used; and 2. Include compensating processes and procedures implemented to provide the ability to uniquely attribute account user activities.
Discussion Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts. Shared and group accounts do not: - Provide the necessary accountability (such as non-repudiation) required to log and monitor access to sensitive information; - Permit identification of individuals who have a need for access;

- Provide audit trails capable of associating a user with an action—eliminating the ability to establish non-repudiation.

Refer to RMH for account management process and procedures.

Implementation Standard

Control Review Frequency	Assessment Frequency
Not Specified	Three (3) Years

Related Controls	Reference Policy

AC-14;	Code: 5 U.S.C. §552a(b)(1), §552a(c)(1);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-3, AS-2;
	HIPAA: 45 AD6C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.308(a)(4)(ii)(C), 45 C.F.R. §164.310(a)(2)(iii), 45 C.F.R. §164.310(b), 45 C.F.R. §164.312(a)(1), 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(a)(2)(ii), 45 C.F.R. §164.312(a)(2)(iv);
	OMB Circular: A-130 7.g. and 8.a.1, 8.b.(2)(c);

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Access to PII is more effectively controlled when access controls are considered during system design and built-into or enforced by the system (i.e., automated controls). Shared and group accounts that do not allow for uniquely attributing user activities should not be used for systems that contain PII or PHI. Shared and group accounts do not allow for the necessary accountability (such as non-repudiation) required to log and monitor access to PII and PHI nor do they permit identification of individuals who have a need for access.

Shared and group accounts do not permit audit trails to associate a user with an action, eliminating the ability to establish non-repudiation. Non-repudiation is a critical element of accountability and accuracy of information in systems, database or system history, and related logs and is important for investigating privacy incidents and breaches.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
AC-02(11)	**Usage Conditions**	**P1**	**High**

Control Statement

Enforce defined circumstances and/or usage conditions (as defined in applicable security and privacy plans) for defined system accounts (as defined in applicable security and privacy plans) .

Discussion

Specifying and enforcing usage conditions helps to enforce the principle of least privilege, increase user accountability, and enable effective account monitoring. Account monitoring includes alerts generated if the account is used in violation of organizational parameters. Organizations can describe specific conditions or circumstances under which system accounts can be used, such as by restricting usage to certain days of the week, time of day, or specific durations of time.

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)

Related Controls	Reference Policy
None;	OMB Memo: M-16-04, M-19-03;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number AC-02(12)	Control Name Account Monitoring for Atypical Usage	Priority P1	CMS Baseline High

Control Statement

(a) Monitor system accounts for atypical use; and

(b) Report atypical usage of system accounts to defined personnel or roles (in applicable security and privacy plans), and if necessary, any applicable incident response team(s).

Discussion

Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress. Account monitoring may inadvertently create privacy risks since data collected to identify atypical usage may reveal previously unknown information about the behavior of individuals. Organizations assess and document privacy risks from monitoring accounts for atypical usage in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Implementation Standard

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls
AU-6, AU-7, CA-7, IR-8, SI-4;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	OMB Memo: M-16-04, M-19-03;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **AC-02(13)**	**Control Name** **Disable Accounts for High-Risk Individuals**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement

Disable accounts of individuals, within the following time-frames, after discovery of individual posing as a significant risk.

(a) Immediately, not to exceed 30 minutes, for systems categorized under FIPS 199 with a security categorization of High; and

(b) Within 60 minutes for systems not categorized under FIPS 199 as having a security categorization of Moderate.

Discussion

Users who pose a significant security and/or privacy risk include individuals for whom reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes adverse impacts to organizational operations, organizational assets, individuals, other organizations, or the Nation. Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.

Implementation Standard

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls
AU-6, SI-4;
	Reference Policy
	Code: 5 U.S.C. §552a(e)(9)-(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(B), 45 C.F.R. §164.308(a)(1)(ii)(C), 45 C.F.R. §164.308(a)(3)(ii)(C);
	OMB Memo:M-16-04, M-17-12, M-19-03;

	[SP 800-162], [SP 800-178], [SP 800-192]

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): Disabling accounts for high-risk individuals is a minimum requirement for the Mission/Business/System's rules of behavior because of abusing access privileges to sensitive information, including information protected under the Privacy Act of 1974.
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **AC-03**	**Control Name** **Access Enforcement**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**

Control Statement Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
Discussion Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family. Well-designed, automated access controls (e.g., mandatory access control [MAC], discretionary access control [DAC], role-based access control [RBAC], or attribute-based access control [ABAC]) limit user access to information per defined access policies, which helps ensure the security and confidentiality of sensitive information contained in the system. FIPS 140-2/140-3 validated modules are listed at: HYPERLINK "https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search"
Implementation Standard High, Moderate & Low: Std.1 - If encryption is used as an access control mechanism, it must meet CMS approved (FIPS 140-2/140-3 compliant and a NIST validated module) encryption standards (see SC-13). Std.2 - Configure operating system controls to disable public "read" and "write" access to all system-related files, objects, and directories as well as files, objects, and directories that contain sensitive information. Std.3 - Data stored in the system must be protected with system access controls and must be encrypted when residing in non-secure areas.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17 , SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31
	Reference Policy
	Code: 5 U.S.C. §552a(b), §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FIPS: 140-2, 140-3;
	FISCAM: AC-3, AC-3.1.5, AC-3.1.6, AC-4.1.1, AS-2, AS-3.8.1;
	HIPAA: 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.308(a)(4)(ii)(C), 45 C.F.R. §164.310(a)(2)(iii), 45 C.F.R. §164.310(b), 45 C.F.R. §164.312(a)(1), 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(a)(2)(ii), 45 C.F.R. §164.312(a)(2)(iv);
	NISTIR: 7874;

	PRIVACT
	NIST SP: 800-57-1, 800-57-2, 800-57-3, 800-162, 800-178;
	OMB Circular: A-130;
	OMB Memo: M-06-16;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a) Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies;
(b) Approved authorizations for logical access to system and resources or external systems should have a level of protection commensurate with the confidentiality, integrity, and availability impact levels of the information being shared versus relying on access control policies;
(c) The external entity must provide a copy of the Authorization to Operate (ATO) for the system that will process, store, or transmit the HVA information. The ATO must be current and signed.

HVA Discussion

Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational HVAs. In addition to enforcing authorized access at the HVA system level and recognizing that systems can host many applications and services in support of missions and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
AC-03(09)	**Controlled Release**	**P3**	**HVA**

Control Statement

Release information outside of the system only if:
(a) The receiving system/system component or external entity (i.e., department, agency, or commercial entity not managed by CMS) provides controls commensurate with those implemented by CMS; and
1. Information is released externally only for the authorized purposes, or in a manner compatible with those purposes, identified in applicable documentation;
(b) CMS-defined controls (defined in applicable security/privacy plans) are used to validate the appropriateness of the information designated for release.

Discussion

Organizations can only directly protect information when it resides within the system. Additional controls may be needed to ensure that organizational information is adequately protected once it is transmitted outside of the system. In situations where the system is unable to determine the adequacy of the protections provided by external entities, as a mitigating control, organizations procedurally determine whether the external systems are providing adequate controls. The means used to determine the adequacy of controls provided by external systems include conducting periodic assessments (inspections/tests), establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received need not be the same as those used by the organization, but the means employed are sufficient to provide consistent adjudication of the security and privacy policy to protect the information and individuals' privacy.
Controlled release of information requires systems to implement technical or procedural means to validate the information prior to releasing it to external systems. For example, if the system passes information to a system controlled by another organization, technical means are employed to validate that the security and privacy attributes associated with the exported information are appropriate for the receiving system. Alternatively, if the system passes information to a printer in organization-controlled space, procedural means can be employed to ensure that only authorized individuals gain access to the printer.

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**
CA-3, PT-7, PT-8, SA-9, SC-16;	Code: 5 U.S.C. §552a(a)(7), §552a(b), §552a(c), §552a(e)(3)(c), §552a(o);

	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208;
	Privacy: Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment, Overview;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Release information outside of the system only if: (a) The receiving system/system component or external entity (i.e., department, agency, or commercial entity not managed by CMS) provides controls commensurate with those implemented by CMS; and 1. Information is released externally only for the authorized purposes, or in a manner compatible with those purposes, identified in applicable documentation; (b) CMS-defined controls (defined in applicable security/privacy plans) are used to validate the appropriateness of the information designated for release. (c) Procedures for sharing or releasing information outside the HVA authorization boundary protect the information through agreements. (d) Limit the sharing of information to only the attributes required by the receiving entity. (e) Perform a risk assessment on the reduced dataset to determine the level of risk and level of protection required to protect the information. (f) Consider validating effective implementation of security protections through technical reviews or inspections of the external entities systems. (g) The external system provides a level of protection commensurate with the confidentiality, integrity, and availability impact levels of the information being shared. (h) The external entity provides a copy of the Authorization to Operate (ATO) for the system that will process, store, or transmit the HVA information and the ATO is current and signed.	
HVA Discussion In situations where the HVA is unable to determine the adequacy of the protections provided by external entities, as a mitigating control, organizations should determine procedurally whether the external systems are providing adequate controls. The means used to determine the adequacy of controls provided by external systems include conducting periodic assessments (inspections/tests), establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received does not need to be the same as those used by the organization, but the means employed are sufficient to provide consistent adjudication of the security and privacy policy to protect the information and individuals' privacy. The external entity should provide a copy of the authorization to operate for the system that will process, store, or transmit the HVA information. The ATO should be current and signed.	
HVA Implementation Standard	

Control Number **AC-03(11)**	**Control Name** **Restrict Access to Specific Information Types**	**Priority** **P2**	**CMS Baseline** **Above Baseline**
Control Statement Restrict access to data repositories containing CMS-defined information types.			
Discussion Restricting access to specific information is intended to provide flexibility regarding access control of specific information types within a system. For example, role-based access could be employed to allow access to only a specific type of personally identifiable information within a database rather than allowing access to the database in its entirety. Other examples include restricting access to cryptographic keys, authentication information, and selected system information.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls CM-8, CM-12, CM-13, PM-5		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number	Control Name	Priority	CMS Baseline
AC-03(14)	**Individual Access**	**P2**	**Moderate** **High**

Control Statement

Provide defined mechanisms (defined in applicable security/privacy plans) to enable individuals to have access to the defined elements of their personally identifiable information (defined in applicable security/privacy plans).

Discussion

Individual access affords individuals the ability to review personally identifiable information about them held within organizational records, regardless of format. Access helps individuals to develop an understanding about how their personally identifiable information is being processed. It can also help individuals ensure that their data is accurate. Access mechanisms can include request forms and application interfaces. For federal agencies, [PRIVACT] processes can be located in systems of record notices and on agency websites. Access to certain types of records may not be appropriate (e.g., for federal agencies, law enforcement records within a system of records may be exempt from disclosure under the [PRIVACT]) or may require certain levels of authentication assurance. Organizational personnel consult with the senior agency official for privacy and legal counsel to determine appropriate mechanisms and access rights or limitations.

It must also be noted that individuals are not always entitled to access to information compiled in reasonable anticipation of a civil action or proceeding. For other examples where agencies may promulgate rules exempting systems from the access provision, see the Privacy Act at 5 USC § 552a, subsections (j) (General Exemptions) and (k) (Specific Exemptions).

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**
IA-8, PM-22, PM-20, PM-21	See Control AC-3;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

The Individual Participation Fair Information Practice Principles (FIPP) requires CMS and CMS Businesses/Systems to provide mechanisms for individuals to gain access to their PII when appropriate. The Privacy Act of 1974, as amended, requires CMS and CMS Businesses/Systems to provide mechanisms for individuals to gain access to their PII when that PII meets the definition of a “record.” Access is also an important aspect of supporting correction of PII and redress against alleged violations and misuse of their PII. In addition to access requirements under the Privacy Act of 1974, as amended, HIPAA has statutory requirements to provide access to PHI.

CMS and CMS Businesses/Systems must provide for public access to records, including PII not included in a Privacy Act System of Records, where required or appropriate. While the language of this control is specific to the Privacy Act’s requirements for access, FIPPs encourage CMS and CMS Businesses/Systems to use available authorities to provide access when the Privacy Act does not apply. For example, CMS Businesses/Systems may use the Freedom of Information Act as another tool to provide access to PII for an affected individual.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Provide authorized individuals with the ability to access their PII maintained in the system's system(s) of records;

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
AC-04	**Information Flow Enforcement**	**P1**	**Moderate** **High** **HVA**

Control Statement

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on defined information flow control policies (in applicable security and privacy plan).

Discussion

Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between connected systems. Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e., allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 32 primarily address cross-domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf products. Information flow enforcement also applies to control plane traffic (e.g., routing and DNS).

Implementation Standard

High & Moderate:

Std.1 - The CMS CIO, CISO, and SOP have the authority to order the immediate termination and/or suspension, within 1 hour, of any interconnection that, in the judgment of the CMS officer and CMS Security Operations, present an unacceptable level of risk to the CMS enterprise and/or mission.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years

Related Controls
AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31;
	Reference Policy
	Code: 5 U.S.C. §552a(b);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-1, AC-1.1.1, AC-1.1.2, AS-2;
	HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.310(b);
	NIST SP: 800-47, 800-160 v1, 800-162, 800-178;
	IR 8112;
	OMB Memo: M-17-12;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

Enforce approved authorizations for controlling the flow of information at the authorization boundary using boundary protection devices (e.g. gateway, router, guard, encrypted tunnel, firewall, application proxy etc.) or at tiered points within the authorization boundary.

HVA Discussion

Information flow control regulates where information can travel within a system and between systems (in contrast to who may access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced

(see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces risk that such transfers violate one or more domain security or privacy policies.
HVA Implementation Standard

Control Number **AC-04(04)**	**Control Name** **Flow Control of Encrypted Information**	**Priority**	**CMS Baseline** **High**
Control Statement Prevent encrypted information from bypassing information flow control mechanisms by either blocking the flow of the encrypted information or terminating communications sessions attempting to pass encrypted information.			
Discussion Flow control mechanisms include content checking, security policy filters, and data type identifiers. The term encryption is extended to cover encoded data not recognized by filtering mechanisms.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	
Related Controls SI-4;		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-05**	**Control Name** **Separation of Duties**	**Priority** **AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8, SA-17;**	**CMS Baseline** **Moderate** **High** **HVA**
Control Statement (a) Identify and document duties of individuals requiring separation; and (b) Define system access authorizations to support separation of duties.			
Discussion P1			
Implementation Standard High: Std.1 - Audit functions must not be performed by security personnel responsible for administering access control. Std.2 - Maintain a limited group of administrators with access based upon the users' roles and responsibilities. Std.3 - The critical mission functions and system support functions must be divided among separate individuals. Std.4 - The system testing functions (i.e., user acceptance, quality assurance, information security) and production functions must be divided among separate individuals or groups. Std.5 - An independent entity, not the Business Owner, ISSO, System Developer(s)/Maintainer(s), or System administrator(s) responsible for the system, conducts information security testing of the system. Std.6 - The quality assurance and code reviews of custom-developed applications, scripts, libraries, and extensions must be conducted by an independent entity rather than the code developers. Moderate: Std.1 - Audit functions must not be performed by security personnel responsible for administering access control.			

Std.2 - Maintain a limited group of administrators with access based upon the users’ roles and responsibilities.
Std.3 - The critical mission functions and system support functions must be divided among separate individuals.
Std.4 - The system testing functions (i.e., user acceptance, quality assurance, information security) and production functions must be divided among separate individuals or groups.
Std.5 - An independent entity, not the Business Owner, ISSO, System Developer(s)/Maintainer(s), or System administrator(s) responsible for the system, conducts information security testing of the system.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
Code: 5 U.S.C. §552a(e)(9)-(10);
Statute: Privacy Act of 1974 (P.L. 93-579);
FedRAMP: Rev. 4 Baseline;
FISCAM: AS-4, SD-1, SD-1.1.1, SD-1.1.3, SD-2, SD-2.1.1, SD-2.2.2, SD-2.2.3, AS-4.4.1, AS-4.4.2;
HIPAA: 45 C.F.R. §164.308(a)(3)(i), 164.308(a)(4)(i),
	Reference Policy

Privacy Discussion
(a) Identify and document duties of individuals requiring separation; and
(b) Define HVA system access authorizations to support separation of duties.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard
Employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations should consider the creation of additional processes, roles, and accounts as necessary, to achieve least privilege. Organizations should apply least privilege to the development, implementation, and operation of organizational systems.

Control Number	Control Name	Priority	CMS Baseline
AC-06	**Least Privilege**	**P1**	**Moderate** **High** **HVA**

Control Statement
Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks in accordance with CMS missions and business functions.

Discussion
Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.
At CMS, the concept of least privilege aligns with the notion of limiting access to CMS's sensitive information to those individuals with a documented need-to-know in performance of their job duties.

Implementation Standard
High & Moderate:
Std.1 - Disable all file system access not explicitly required for system, application, and administrator functionality.
Std.2 - Contractors must be provided with minimal system and physical access, and must agree to and support the CMS security requirements. The contractor selection process must assess the contractor’s ability to adhere to and support CMS security policy.

Std.3 - Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control. Std.4 - Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties. Std.5 - Disable all system and removable media boot access unless it is explicitly authorized by the CIO for compelling operational needs. If system and removable media boot access is authorized, boot access is password protected.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38;
	Reference Policy
	Code: 5 U.S.C. §552a(b);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-3, AS-2;
	HIPAA: 45 C.F.R. §164.308(a)(3)(i), 45 C.F.R. §164.308(a)(4)(i), 45 C.F.R. §164.502(b), 45 C.F.R. §164.308(a)(4)(ii)(A), 45 C.F.R. §164.312(a)(1);
	HSPD: HSPD-7 D(10);
	OMB Circular: A-130;
	OMB Memo: M-06-16;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AC-06(01)**	**Control Name** **Authorize Access to Security Functions**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Authorize access for defined individuals or roles to: (a) CMS -defined security functions (deployed in hardware, software, and firmware); and (b) CMS-defined security-relevant information, including but not limited to: 1. Setting/modifying audit logs and auditing behavior; 2. Setting/modifying boundary protection system rules; 3. Configuring/modifying access authorizations (i.e., permissions, privileges); 4. Setting/modifying authentication parameters; and 5. Setting/modifying system configurations and parameters.			
Discussion Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.			
Implementation Standard			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	
Related Controls		**Reference Policy**	

AC-17, AC-18, AC-19, AU-9, PE-2;	Code: 5 U.S.C. §552a(b)(1);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	HIPAA: 45 C.F.R. §164.308(a)(3)(i), 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(3)(ii)(B), 45 C.F.R. §164.308(a)(4)(i), 45 C.F.R. §164.502(b);
	OMB Memo: M-06-16;

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): Limiting access to security functions to authorized personnel reduces the number of users able to perform certain security functions, such as configuring access permissions, setting audit logs, performing system management functions. Examples of authorized personnel include security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. These types of security functions can provide a level of access to PII, and capabilities to manipulate it, in ways that other users' roles typically could not. The CMS Business/System identifies the security relevant functions that require authorized access for all systems that contain moderate or high PII confidentiality impact level information.
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
AC-06(02)	**Non-privileged Access for Nonsecurity Functions**	**P1**	**Moderate** **High**

Control Statement (a) Require that users of system accounts (or roles) with access to CMS-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing nonsecurity functions. The following list of CMS-defined security functions or security-relevant information include, but are not limited to : 1. Setting/modifying audit logs and auditing behavior; 2. Setting/modifying boundary protection system rules; 3. Configuring/modifying access authorizations (i.e., permissions, privileges); 4. Setting/modifying authentication parameters; and 5. Setting/modifying system configurations and parameters.
Discussion Requiring the use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies, such as role-based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.
Implementation Standard

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AC-17, AC-18, AC-19, PL-4;
	Reference Policy
	Code: 5 U.S.C. §552a(b);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(B), 45 C.F.R. §164.502(b);
	OMB Memo: M-06-16;

<table>
<tr><td><b>Privacy Discussion</b></td></tr>
<tr><td><b>Privacy Implementation Standards</b></td></tr>
<tr><td><b>HVA Control Statement</b></td></tr>
<tr><td><b>HVA Discussion</b></td></tr>
<tr><td><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
AC-06(03)</td><td colspan="2"><b>Control Name</b>
Network Access to Privileged Commands</td><td><b>Priority</b>
P1</td><td><b>CMS Baseline</b>
High</td></tr>
<tr><td colspan="5"><b>Control Statement</b>
Authorize network access to privileged commands only for compelling operational needs as defined in applicable security and privacy plans and document the rationale for such access in applicable security and privacy plans for the system.</td></tr>
<tr><td colspan="5"><b>Discussion</b>
Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device).
CMS limits network access to activities requiring elevated privileges to situations where there is a compelling operational need. For example, a compelling operational need could include routine administration (management) of remote security and infrastructure devices across a dedicated management network (see the TRA).</td></tr>
<tr><td colspan="5"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Quarterly</td><td colspan="3"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
AC-17, AC-18, AC-19;</td><td colspan="3"><b>Reference Policy</b>
Code: 5 U.S.C. §552a(b)(1);
Statute: Privacy Act of 1974 (P.L. 93-579);
OMB Memo: M-06-16;</td></tr>
<tr><td colspan="5"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="5"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="5"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="5"><b>HVA Discussion</b></td></tr>
<tr><td colspan="5"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
AC-06(05)</td><td colspan="2"><b>Control Name</b>
Privileged Accounts</td><td><b>Priority</b>
P1</td><td><b>CMS Baseline</b>
Moderate
High
HVA</td></tr>
<tr><td colspan="5"><b>Control Statement</b>
Restrict privileged accounts on the system to personnel or roles (defined in applicable security and privacy plans).</td></tr>
<tr><td colspan="5"><b>Discussion</b>
Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.</td></tr>
<tr><td colspan="5"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Quarterly</td><td colspan="3"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
IA-2, MA-3, MA-4;</td><td colspan="3"><b>Reference Policy</b>
Code: 5 U.S.C. §552a(b)(1);
Statute: Privacy Act of 1974 (P.L. 93-579);
FedRAMP: Rev. 4 Baseline;</td></tr>
</table>

	HIPAA: 45 C.F.R. §164.308(a)(3)(i), 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(3)(ii)(B), 45 C.F.R. §164.312(a)(1);
	OMB Circular: A-130;
	OMB Memo: M-06-16;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement (a) Restrict privileged accounts on the system to personnel or roles (defined in applicable security and privacy plans). (b) Disallow access to other networks or systems outside the authorization boundary (i.e. the Internet, other internal systems) by accounts with elevated privileges. (c) Restrict and limit rights to functions, services, and attributes on accounts with elevated privileges to those necessary to perform the required tasks.	
HVA Discussion Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off the shelf (COTS) operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided they retain the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.	
HVA Implementation Standard	

Control Number AC-06(06)	**Control Name** Privileged Access by Non-Organizational Users	**Priority**	**CMS Baseline** Above Baseline
Control Statement Prohibit privileged access to the system by non-organizational users.			
Discussion An organizational user is an employee or an individual considered by the organization to have the equivalent status of an employee. Organizational users include contractors, guest researchers, or individuals detailed from other organizations. A nonorganizational user is a user who is not an organizational user. Policies and procedures for granting equivalent status of employees to individuals include a need-to-know, citizenship, and the relationship to the organization.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls AC-18, AC-19, IA-2, IA-8		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-06(07)**	**Control Name** **Review of User Privileges**	**Priority** **P3**	**CMS Baseline** **Moderate** **High** **HVA**
Control Statement (a) Review no less often than every ninety (90) days the privileges assigned to defined roles or classes of users to validate the need for such privileges; and (b) Reassign or remove privileges, if necessary, to correctly reflect CMS' mission and business needs.			

Discussion The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
CA-7;
	Reference Policy
	Code: 5 U.S.C. §552a(b), §552a(e)(9)-(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(3)(ii)(B), 45 C.F.R. §164.308(a)(4)(i), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.308(a)(4)(ii)(C), 45 C.F.R. 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(a);
	OMB Circular: A-130;
	OMB Memo: M-17-12;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement (a) Review no less often than every ninety (90) days the privileges assigned to defined roles or classes of users to validate the need for such privileges; as well as conduct quarterly reviews of the rights assigned to privileged accounts and validate the need for such privileges. (b) Reassign or remove privileges, if necessary, to correctly reflect CMS' mission and business needs.	
HVA Discussion The need for certain assigned user privileges may change over time reflecting changes in organizational missions and business functions, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations should take appropriate corrective actions. HVA account reviews may be conducted on a more frequent basis due to the sensitivity of the HVA system and information.	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
AC-06(09)	**Log Use of Privileged Functions**	**P1**	**Moderate** **High**
Control Statement Log the execution of privileged functions.			
Discussion The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and, in doing so, help mitigate the risk from insider threats and the advanced persistent threat.			
Implementation Standard			
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years		

Related Controls
AU-2, AU-3, AU-12;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R.§164.312(b);
	OMB Circular: A-130 7.g. and Appendix III;		

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **AC-06(10)**	**Control Name** **Prohibit Non-privileged Users from Executing Privileged Functions**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement Prevent non-privileged users from executing privileged functions.
Discussion Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. Preventing non-privileged users from executing privileged functions is enforced by AC-3.
Implementation Standard

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
None;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	OMB Circular: A-130 7.g. and Appendix III;

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **AC-07**	**Control Name** **Unsuccessful Logon Attempts**	**Priority** **P2**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement (a) Enforce a limit of consecutive invalid login attempts by a user, specified in Implementation Standard 1, during a duration specified in Implementation Standard 1; and (b) Automatically disable or lock the account or node for the time period specified in Implementation Standard 1 or until the lock is released by an administrator, and record the event within appropriate security logs when the maximum number of unsuccessful attempts is exceeded.
Discussion The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined, organization-defined time period. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels. Organization-defined actions that may be taken when the number of allowed consecutive invalid logon attempts is exceeded include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only logon from specified Internet Protocol (IP)

addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address. If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, organizations consider a combination of other actions to help prevent brute force attacks. In addition to the above, organizations can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or need.	
Implementation Standard High: Std.1 - Configure the system to lock out the user account automatically after three (3) invalid login attempts during a 120-minute time window. Require the lock out to persist until released by an administrator. Moderate: Std.1 - Configure the system to lock out the user account automatically after five (5) invalid login attempts during a 120-minute time window. Require the lock out to persist for a minimum of one (1) hour. Low: Std.1 - Configure the system to disable access for at least fifteen (15) minutes after five (5) invalid login attempts during a 120-minute time window.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-2, AC-9, AU-2, AU-6, IA-5;
	Reference Policy
	FedRAMP: Rev. 4 Baseline; 7
	FISCAM: AC-2, AC-2.1.7, AS-2;
	NIST SP: 800-63-3, 800-124;
	OMB M-16-04, M-19-03;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AC-07(02)**	**Control Name** **Purge or Wipe Mobile Device**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Purge or wipe information from mobile devices based on NIST Special Publication R1 – Guidelines for Media Sanitization after five consecutive, unsuccessful device logon attempts.			
Discussion A mobile device is a computing device that has a small form factor such that it can be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Purging or wiping the device applies only to mobile devices for which the organization-defined number of unsuccessful logons occurs. The logon is to the mobile device, not to any one account on the device. Successful logons to accounts on mobile devices reset the unsuccessful logon count to zero. Purging or wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.			
Implementation Standard			
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years		
Related Controls AC-19, MP-5, MP-6 SC-13	**Reference Policy**		
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			

Control Number	Control Name	Priority	CMS Baseline
AC-08	**System Use Notification**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Display an approved system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. The approved CMS banner states:

* This warning banner provides privacy and security notices consistent with applicable federal laws, directives, and other federal guidance for accessing this Government system, which includes (1) this computer network, (2) all computers connected to this network, and (3) all devices and storage media attached to this network or to a computer on this network.

* This system is provided for Government authorized use only.

* Unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties.

* Personal use of social media and networking sites on this system is limited as to not interfere with official work duties and is subject to monitoring.

* By using this system, you understand and consent to the following:

- The Government may monitor, record, and audit your system usage, including usage of personal devices and email systems for official duties or to conduct HHS business. Therefore, you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this system.
- Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose

(b) Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

(c) For publicly accessible systems:

1. Display system use information describing CMS-defined permitted uses, before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

Discussion

System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon interfaces with human users. Notifications are not required when human interfaces do not exist. Based on an assessment of risk, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network logon. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users. Organizations consult with the privacy office for input regarding privacy messaging and the Office of the General Counsel or organizational equivalent for legal review and approval of warning banner content.

The warning banner language has very important legal implications for CMS and its system resources. Should content need to be added to this banner, submit the modified warning banner language to the CMS CIO for review and approval prior to implementation. If an system has character limitations related to the warning banner display, the CMS CIO can provide an abbreviated warning banner version. If this banner is inconsistent with any directives, policies, regulations, or standards, notify the CMS CIO immediately.

All system computers and network devices under CMS control, prominently display the notice and consent banner immediately upon users' authentication to the system, including, but not limited to, websites, web pages where substantial personal information from the public is collected, Secure File Transfer Protocol (SFTP), Secure Shell (SSH), or other services accessed.

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

AC-14, PL-4, SI-4;	Code: 5 U.S.C. §552a(e)(3), §552a(e)(4);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;

	FISCAM: AC-1, AS-2;
	HHS: Policy for Monitoring Employee Use of HHS IT Resources;
	HIPAA: 45 C.F.R. §164.520(1)(i);
	OMB Circular: A-130 7.g.;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AC-09**	**Control Name** **Previous Logon Notification**	**Priority** **P3**	**CMS Baseline** **Above Baseline**
Control Statement When supported by the underlying operating system, notify the user, upon successful logon to the system, of the date and time of the last logon.			
Discussion Previous logon notification is applicable to system access via human user interfaces and access to systems that occurs in other types of architectures. Information about the last successful logon allows the user to recognize if the date and time provided is not consistent with the user's last access.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls AC-7, PL-4;		**Reference Policy** FISCAM: AC-1, AS-2;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-09(01)**	**Control Name** **Unsuccessful Logons**	**Priority** **P3**	**CMS Baseline** **Above Baseline**
Control Statement When supported by the underlying operating system, notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.			
Discussion Information about the number of unsuccessful logon attempts since the last successful logon allows the user to recognize if the number of unsuccessful logon attempts is consistent with the user's actual logon attempts. Due to the possibility that an unauthorized person could logon to a system or application using an authorized person's logon account and credentials, all systems and applicable applications will provide an automated method of notifying the authorized user of the last successful logon date and time, and the number of previously unsuccessful logon attempts. It is important that training include reporting procedures and responsibility for authorized users to report unauthorized logons and unauthorized attempts to logon.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None;		**Reference Policy** See Control AC-9;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			

HVA Implementation Standard

Control Number **AC-10**	**Control Name** **Concurrent Session Control**	**Priority** **P3**	**CMS Baseline** **High**
Control Statement Limit the number of concurrent sessions for each account and/or account types to one (1) session for both normal and privileged users. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one (1) concurrent application/process session is documented in the applicable security and privacy plan.			
Discussion Organizations may define the maximum number of concurrent sessions for system accounts globally, by account type, by account, or any combination thereof. For example, organizations may limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications. Concurrent session control addresses concurrent sessions for system accounts. It does not, however, address concurrent sessions by single users via multiple system accounts.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
SC-23;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		FISCAM: AC-2, AS-2;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-11**	**Control Name** **Device Lock**	**Priority** **P3**	**CMS Baseline** **Moderate** **High**
Control Statement (a) Prevent further access to the system by initiating a device lock after fifteen (15) minutes of inactivity (for both remote and internal access connections), requiring the user to initiate a device lock before leaving the system unattended, or upon receiving a request from a user; and (b) Retain the device lock until the user reestablishes access using established identification and authentication procedures.			
Discussion Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User-initiated device locking is behavior or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.			
Implementation Standard High & Moderate: Std.1 - Period of inactivity must be no more than 15 minutes before device lock occurs for remote and mobile devices and requires user re-authentication. As agencies continue to migrate to laptops and docking stations making clients increasingly mobile, this is a logical extension of that requirement.			

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AC-2, AC-7, IA-11, PL-4;
	Reference Policy
	Code: 5 U.S.C. §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-1, AC-1.2.1, AS-2;
	HIPAA: 45 C.F.R. §164.310(b), 45 C.F.R. §164.312(a)(2)(iii), 45 C.F.R. §164.312(a)(1);
	OMB Memo: M-06-16, M-17-12;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AC-11(01)**	**Control Name** **Pattern-hiding Displays**	**Priority** **P3**	**CMS Baseline** **Moderate** **High**
Control Statement Conceal, via the device lock, information previously visible on the display with a publicly viewable image.			
Discussion The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.			
Implementation Standard			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	
Related Controls None;		**Reference Policy** FedRAMP: Rev. 4 Baseline;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-12**	**Control Name** **Session Termination**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**
Control Statement Automatically terminate a user session after defined conditions or trigger events requiring session disconnect (defined in applicable security and privacy plans)			
Discussion			

Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions (i.e., network disconnect)). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls MA-4, SC-10, SC-23;	**Reference Policy** FISCAM: AC-1.2.1;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
AC-14	**Permitted Actions Without Identification or Authentication**	**P3**	**Low** **Moderate** **High**

Control Statement (a) Identify specific user actions (defined in applicable security and privacy plans) that can be performed on the system without identification or authentication consistent with CMS' missions and business functions; (b) Document and provide supporting rationale in the security and privacy plan for the system, user actions not requiring identification or authentication.	
Discussion Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication are not required for the specified user actions. Organizations may allow a limited number of user actions without identification or authentication, including when individuals access public websites or other publicly accessible federal systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations identify actions that normally require identification or authentication but may, under certain circumstances, allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. Permitting actions without identification or authentication does not apply to situations where identification and authentication have already occurred and are not repeated but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication, and therefore, the value for the assignment can be "none."	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-8, IA-2, PL-2;
	Reference Policy
	Code: 5 U.S.C. §552a(b);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-1.1.7, AC-2, AC-3.2.5, AS-2;
	HIPAA: 45 C.F.R. §164.312(a)(2)(i);
	OMB Circular: A-130 7.g. and Appendix III;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	

HVA Discussion
HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
AC-17	**Remote Access**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

(a) Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
(b) Authorize each type of remote access to the system prior to allowing such connections.
1. Remote access for privileged functions must be permitted only for compelling operational needs, must be strictly controlled, and must be explicitly authorized, in writing, by the Authorizing Official (AO) or his/her designated representative.
(c) While access to HHS Webmail using personally-owned equipment is authorized, access to other systems/networks using personally-owned equipment is prohibited without written authorization from the Authorizing Official (AO), or an approved security and privacy policy allowing the use of personally-owned equipment:
1. Personally-owned equipment must be scanned before being connected to CMS (and HHS) systems or networks to ensure compliance with CMS requirements; and
2. Personally-owned equipment must be prohibited from processing, accessing, or storing Department sensitive information unless it is approved in writing by the CMS SOP and employs CMS required encryption (FIPS 140-2/140-3 validated module).

Discussion

Remote access is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the ability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. Authorization of each remote access type addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use information exchange and system connection security agreements to manage remote access connections to other systems, such agreements are addressed as part of CA-3. Enforcing access restrictions for remote access is addressed via AC-3.

Implementation Standard

High, Moderate & Low:
Std.1 - Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi-Protocol Label Switching (MPLS) service network cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor will be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified within every three hundred sixty-five (365) days.
Std.2 - If e-authentication is implemented as a remote access solution or associated with remote access.
Std.3 - All computers and devices, whether government furnished equipment (GFE), contractor furnished equipment (CFE), or personal, that require any network access to a CMS network or system are securely configured and meet, as a minimum, the following security requirements:
(a) Up-to-date system patches;
(b) Current anti-virus software;
(c) Host-based intrusion detection system;
(d) Functionality that provides the capability for automatic execution of code disabled; and
(e) employs CMS required encryption (FIPS 140-2/140-3 validated module).
Std.4 - For organizations supporting remote access (including teleworking), ensure NIST SP 800-46 guidelines are followed by defining policies and procedures that define:
(a) Forms of permitted remote access;
(b) Types of devices permissible for remote access;
(c) Type of access remote users are granted; and

(d) How remote user account provisioning is handled.

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-1, AC-1.1.4, AC-1.1.5, AC-1.1.6, AC-1.1.7, AS-2;
	HIPAA: 45 C.F.R. §164.310(b), 45 C.F.R. §164.310(c), 45 C.F.R. §164.312(a)(1), 45 C.F.R. §164.312(e)(1);
	NISTIR: 7966;
	NIST SP: 800-46, 800-77, 800-113, 800-114, 800-121;
	OMB Circular: A-130;
	OMB Memo: M-06-16, M-17-12;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a) Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

(b) Authorize each type of remote access to the system prior to allowing such connections.

1. Remote access for privileged functions must be permitted only for compelling operational needs, must be strictly controlled, and must be explicitly authorized, in writing, by the Authorizing Official (AO) or his/her designated representative.

(c) While access to HHS Webmail using personally-owned equipment is authorized, access to other systems/networks using personally-owned equipment is prohibited without written authorization from the Authorizing Official (AO), or an approved security and privacy policy allowing the use of personally-owned equipment:

1. Personally-owned equipment must be scanned before being connected to CMS (and HHS) systems or networks to ensure compliance with CMS requirements; and
2. Personally-owned equipment must be prohibited from processing, accessing, or storing Department sensitive information unless it is approved in writing by the CMS SOP and employs CMS required encryption (FIPS 140-2/140-3 validated module).

(d) Control and limit access to the HVA environment from remote locations (outside the HVA authorization boundary) to pre-authorized remote locations (defined in applicable HVA security/privacy plans).

HVA Discussion

Remote access is access to organizational systems (or processes acting on behalf of users) communicating through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. Remote access into the HVA environment is restricted and controlled at the authorization boundary of the HVA. Entities that leverage enterprise remote access solutions from systems outside the enterprise must further control access at the HVA authorization boundary into the HVA environment over the support systems' network. Likewise, systems outside the HVA authorization boundary but located on a support system's authorization boundary are considered remote access devices to the HVA and must be controlled and limited when accessing the HVA environment.

HVA Implementation Standard

Control Number **AC-17(01)**	**Control Name** **Monitoring and Control**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement

Employ automated mechanisms to monitor and control remote access methods.

Discussion

Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.

<table>
<tr><td colspan="2"><b>Implementation Standard</b>
High & Moderate:
Std.1 - The organization implements CMS and federally distributed blocking rules within one hour of receipt.</td></tr>
<tr><td><b>Control Review Frequency</b>
Quarterly</td><td><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td><b>Related Controls</b>
AU-2, AU-6, AU-12, AU-14;</td><td><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
HIPAA: 45 C.F.R. §164.310(b), 45 C.F.R. §164.310(c), 45 C.F.R. §164.312(a)(1), 45 C.F.R. §164.312(b), 45 C.F.R. §164.312(e)(1);
NIST SP: 800-37, 800-39, 800-137;
OMB Memo: M-06-16, M-14-03, M-16-04, M-17-12, M-19-03, M-20-04;</td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b>
Discussion for systems processing, storing, or transmitting PII (to include PHI):
Auditing remote access ensures unauthorized connections to systems containing personally identifiable information (PII) can be detected across all system platforms (e.g., servers, mobile devices, work stations).
Audit all remote access to, and actions on, resources containing PII.</td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="2"><b>HVA Discussion</b></td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>AC-17(02)</b></td><td><b>Control Name</b>
<b>Protection of Confidentiality and Integrity Using Encryption</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Moderate</b>
<b>High</b>
<b>HVA</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.
Use only CMS-approved encryption mechanisms (e.g., see SC-13).</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
SC-8, SC-12, SC-13;</td><td colspan="2"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
HIPAA: 45 C.F.R. §164.312(a)(2)(iv), 45 C.F.R. §164.312(e)(2)(ii);
OMB Circular: A-130;
OMB Memo: M-06-16, Step 3;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b>
Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access data/sessions by using FIPS 140-2/140-3 compliance encryption.</td></tr>
<tr><td colspan="4"><b>HVA Discussion</b>
Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.</td></tr>
</table>

HVA Implementation Standard

Control Number **AC-17(03)**	**Control Name** **Managed Access Control Points**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Route remote accesses through authorized and managed network access control points.			
Discussion Organizations consider the Trusted Internet Connections (TIC) initiative [DHS TIC] requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.			
Implementation Standard			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	

Related Controls
SC-7;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		OMB Memo: M-16-04, M-19-03, M-19-26;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-17(04)**	**Control Name** **Privileged Commands and Access**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement (a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for compelling operational needs; and (b) Document the rationale for remote access in the security and privacy plan for the system.			
Discussion Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.			
Implementation Standard			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	
Related Controls AC-6, SC-12, SC-13;		**Reference Policy** FedRAMP: Rev. 4 Baseline;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-17(06)**	**Control Name** **Protection of Mechanism Information**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Protect information about remote access mechanisms from unauthorized use and disclosure.			
Discussion Remote access to organizational information by non-organizational entities can increase the risk of unauthorized use and disclosure about remote access mechanisms. The organization considers including remote access requirements in the information exchange agreements with other organizations, as applicable. Remote access requirements can also be included in rules of behavior (see PL-4) and access agreements (see PS-6).			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls AT-2, AT-3, PS-6		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-17(09)**	**Control Name** **Disconnect or Disable Access**	**Priority** **P1**	**CMS Baseline** **Above Baseline**
Control Statement Provide the capability to disconnect or disable remote access to the system within one (1) hour.			
Discussion The speed of system disconnect or disablement varies based on the criticality of missions or business functions and the need to eliminate immediate or future remote access to systems.. CMS Business Owners are to ensure that required Interconnection Security Agreements (ISA) and Memoranda of Understanding (MOU) are established and that they state the interconnections may be terminated or suspended by CMS unilaterally based solely on CMS' interpretation of the risk.			
Implementation Standard High, Moderate & Low: Std.1 - The organization terminates or suspends network connections (i.e., a system to system interconnection) within one (1) hour upon issuance of an order by the CIO, CISO, or Senior Official for Privacy (SOP).			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None;		**Reference Policy** FedRAMP: Rev. 4 Baseline;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number	Control Name	Priority	CMS Baseline
AC-18	**Wireless Access**	**P1**	**Low** **Moderate** **High**

Control Statement

Monitor for unauthorized wireless access to information systems and prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If wireless access is authorized:
(a). Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and
(b). Authorize each type of wireless access to the system prior to allowing such connections.

Discussion

Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols that provide authenticator protection and mutual authentication.

Implementation Standard

High, Moderate & Low:

Std.1 - If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless restrictions and access controls are implemented:

(a) Encryption protection is enabled;
(b) Access points are placed in secure areas;
(c) Access points are shut down when not in use (i.e., nights, weekends);
(d) A stateful inspection firewall is implemented between the wireless network and the wired infrastructure;
(e) MAC address authentication is utilized;
(f) Static IP addresses, not Dynamic Host Configuration Protocol (DHCP), is utilized;
(g) Personal firewalls are utilized on all wireless clients;
(h) File sharing is disabled on all wireless clients;
(i) Intrusion detection agents are deployed on the wireless side of the firewall;
(j) Wireless activity is monitored and recorded, and the records are reviewed on a regular basis (defined in applicable security/privacy plans);
(k) Adheres to CMS-CIO-POL-INF12-01, CMS Policy for Wireless Client Access; and
(l) Adheres to the HHS Standard for IEEE 802.11 Wireless Local Area Network (WLAN).

Std.2 - Wireless printers and all Bluetooth devices such as keyboards are not allowed.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)

Related Controls	Reference Policy

AC-2, AC-3, AC-17, AC-19, CA-9, CM-7, IA-2, IA-3, IA-8, PL-4, SC-40, SC-43, SI-4;	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-1, AS-2;
	HHS: IS2P 2014;
	NIST SP: 800-48, 800-94, 800-97;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

<table>
<tr><td><b>Control Number</b>
AC-18(01)</td><td><b>Control Name</b>
Authentication and Encryption</td><td><b>Priority</b>
P1</td><td><b>CMS Baseline</b>
Moderate
High</td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Protect wireless access to the system using authentication of both users and devices and encryption.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.
Per HHS IS2P policy (2018), compliance with NIST SP 800-153 is required for user authentication and encrypted communications using WPA-2 and NIST SP 800-97 2-factor authentication requirements for WLAN connectivity.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
SC-8, SC-12, SC-13;</td><td colspan="2"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
NIST SP: 800-97, 800-153;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b>
Discussion for systems processing, storing, or transmitting PII (to include PHI):
Communication over wireless networks, unless properly secured, has a greater risk of interception than hard-wired networks. Implementing encryption of wireless network communications containing personally identifiable information (PII) renders any intercepted data unreadable.
If wireless networks permit access to CMS Business/System systems containing PII, then encryption of content and authentication of users or devices is required. CMS Businesses/Systems should ensure that all WLAN components use FIPS-approved cryptographic algorithms to protect the confidentiality and integrity of WLAN communications.</td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
AC-18(03)</td><td><b>Control Name</b>
Disable Wireless Networking</td><td><b>Priority</b></td><td><b>CMS Baseline</b>
Low
Moderate
High</td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
AC-19</td><td colspan="2"><b>Reference Policy</b></td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
</table>

HVA Implementation Standard

Control Number **AC-18(04)**	**Control Name** **Wireless Access | Restrict Configurations by Users**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.			
Discussion Organizational authorizations to allow selected users to configure wireless networking capabilities are enforced, in part, by the access enforcement mechanisms employed within organizational systems. Per HHS IS2P policy (2018), compliance with NIST SP 800-153 is required for restricting user configuration.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls SC-7, SC-15;		**Reference Policy** See Control AC-18;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-18(05)**	**Control Name** **Wireless Access | Antennas and Transmission Power Levels**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of CMS-controlled boundaries.			
Discussion Actions that may be taken to limit unauthorized use of wireless communications outside of organization-controlled boundaries include reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be captured outside of the physical perimeters of the organization, employing measures such as emissions security to control wireless emanations, and using directional or beamforming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such mitigating actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational systems as well as other systems that may be operating in the area. Per HHS IS2P policy (2018), compliance with NIST SP 800-153 is required for calibrating transmission power levels.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls PE-19;		**Reference Policy** See Control AC-18;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-19**	**Control Name** **Access Control for Mobile Devices**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement (a) Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and (b). Authorize the connection of mobile devices to organizational systems.			
Discussion A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending on the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting information and systems. Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware. Usage restrictions and authorization to connect may vary among organizational systems. For example, the organization may authorize the connection of mobile devices to the organizational network and impose a set of usage restrictions, while a system owner may withhold authorization for mobile device connection to specific applications or impose additional usage restrictions before allowing mobile device connections to a system. Adequate security for mobile devices goes beyond the requirements specified in AC-19. Many controls for mobile devices are reflected in other controls allocated to the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some overlap by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-2, IA-3, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SC-34, SC-43, SI-3, SI-4;
		Reference Policy
		FISCAM: AC-1.1.2, CM-2.1.1;
		NIST SP: 800-114, 800-124;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-19(05)**	**Control Name** **Full Device and Container-based Encryption**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Employ CMS-required (FIPS 140-2/140-3 validated module) full-device encryption or container encryption to protect the confidentiality and integrity of information on approved mobile devices (defined in applicable security and privacy plans).			

Discussion Container-based encryption provides a more fine-grained approach to data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields. FIPS 140-2/140-3 approved security function families are found at HYPERLINK "https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation" . However, implementing an approved security function is the start. The product must also be on the approved validation lists. (See HYPERLINK "https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search" for a list of current validated products.)	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
SC-12, SC-13, SC-28;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FIPS: 140-2, 140-3;
	FISCAM: 1.1.4, AC-1.1.5, AC-1.1.6, AC-1.1.7;
	HIPAA: 45 C.F.R. §164.312(a)(2)(iv);
	OMB Memo: M-06-16;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AC-20**	**Control Name** **Use of External Systems**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement (a). Establish defined terms and conditions and identify defined controls asserted to be implemented on external systems, consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1 Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or (b). Prohibit the use of organizationally-defined types of external systems.			
Discussion External systems are systems that are used by but not part of organizational systems and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. External systems include personally owned systems, components, or devices; privately owned computing and communications devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; systems managed by contractors; and federal information systems that are not owned by, operated by, or under the direct supervision or authority of the organization. External systems also include systems owned or operated by other components within the same organization and systems within the organization with different authorization boundaries. Organizations have the option to prohibit the use of any type of external system or prohibit the use of specified types of external systems, (e.g., prohibit the use of any external system that is not organizationally owned or prohibit the use of personally-owned systems). For some external systems (i.e., systems operated by other organizations), the trust relationships that have been established between those organizations and the originating organization may be such that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing information exchange agreements (either implicit or explicit) established between organizations or components or when such agreements are specified by applicable laws, executive orders, directives, regulations, policies, or standards. Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to organizational systems and over which organizations have the authority to impose specific rules of behavior regarding system access.			

Restrictions that organizations impose on authorized individuals need not be uniform, as the restrictions may vary depending on trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

External systems used to access public interfaces to organizational systems are outside the scope of AC-20. Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems. If the terms and conditions with the owners of the external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

For some external systems, those systems operated by other federal agencies, including organizations subordinate to CMS, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the systems of these organizations would not be considered external.

Implementation Standard

High, Moderate & Low:

Std.1 - Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees.

Std.2 - The defined terms and conditions must address, at a minimum:

a. The types of applications that can be accessed from external information systems;
b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
c. How other users of the external information system will be prevented from accessing federal information;
d. The use of VPN and stateful inspection firewall technologies;
e. The use of and protection against the vulnerabilities of wireless technologies;
f. The maintenance of adequate physical security controls;
g. The use of virus and spyware protection software; and
h. How often the security capabilities of installed software are to be updated.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7;	Code: 5 U.S.C. §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FAR: Part 24, 39.105;
	FedRAMP: Rev. 4 Baseline;
	FIPS: 199;
	FISCAM: AS-1, SM-7;
	HHS: IS2P 2014;
	HIPAA: 45 C.F.R. §164.312(a)(2)(i);
	NIST SP: 800-171, 800-172;
	OMB Circular: A-130 7.g.;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a). Establish defined terms and conditions and identify defined controls asserted to be implemented on external systems, consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

1 Access the system from external systems; and
2. Process, store, or transmit organization-controlled information using external systems; or

(b). Prohibit the use of organizationally-defined types of external systems.

(c) Establishes strict terms and conditions for acceptable use, in accordance with documented security and privacy policies and procedures and federal guidelines and laws. The terms and conditions (contractual requirements for vendors/consultants) shall specify:

(1) Types of access allowed into the environment;
(2) Security requirements for the external system; and
(3) Information handling limitations and restrictions.

HVA Discussion

External systems are systems that are used by, but not a part of, organizational systems and for which the organization has no direct control over the implementation of required security and privacy controls or the assessment of control effectiveness.

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
AC-20(01)	**Limits on Authorized Use**	**P1**	**Moderate** **High**

Control Statement

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:
(a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or
(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

Discussion

Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

Implementation Standard

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

CA-2;	Code: 5 U.S.C. §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FAR: Part 24, 39.105;
	FedRAMP: Rev. 4 Baseline;
	HIPAA: 45 C.F.R. §164.314(a);
	OMB Circular: A-130 7.g.;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
AC-20(02)	**Portable Storage Devices — Restricted Use**	**P1**	**Moderate** **High**

Control Statement

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using organization-defined restrictions (defined in applicable security and privacy plans)

Discussion

Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.	
Implementation Standard High & Moderate: Std.1 - Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems unless: (a) The use is documented within appropriate security/privacy plans; (b) Explicitly authorized, in writing, by the Authorizing Official (AO) or his/her designated representative; (c) Personally-owned devices to which CMS-controlled portable storage devices are to be attached comply with HHS and CMS policies and directives on use of personally-owned systems and components; and (d) Security and privacy safeguards are employed that are appropriate for the sensitivity of the data.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls MP-7, SC-41;	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AC-20(03)**	**Control Name** **Non-organizationally Owned Systems — Restricted Use**	**Priority** **P3**	**CMS Baseline** **Above Baseline**
Control Statement Restrict the use of non-organizationally owned (i.e., non-CMS) systems or system components to process, store, or transmit CMS information unless: (a) The use of contractor-owned devices is: 1. Documented within the contract and appropriate security and privacy plans; 2. Explicitly authorized, in writing, by the Authorizing Official (AO) or his/her designated representative; (b)Use of personally owned devices comply with HHS and CMS policies and directives on use of personally-owned systems and components; and (c) Security and privacy safeguards are employed that are appropriate for the sensitivity of the data. (d) Includes implementation of either full-device or virtual container encryption to reduce the vulnerability to CMS sensitive information processed, stored, or transmitted by non-organizationally owned (i.e., non-CMS) systems or system components (devices).			
Discussion Non-organizationally owned systems or system components include systems or system components owned by other organizations as well as personally owned devices. There are potential risks to using non-organizationally owned systems or components. In some cases, the risk is sufficiently high as to prohibit such use (see AC-20(6)). In other cases, the use of such systems or system components may be allowed but restricted in some way. Restrictions include requiring the implementation of approved controls prior to authorizing the connection of non-organizationally owned systems and components; limiting access to types of information, services, or applications; using virtualization techniques to limit processing and storage activities to servers or system components provisioned by the organization; and agreeing to the terms and conditions for usage. Organizations consult with the Office of the General Counsel regarding legal issues associated with using personally owned devices, including requirements for conducting forensic analyses during investigations after an incident.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	

Related Controls		**Reference Policy**
		Code: 5 U.S.C. §552a(e)(10);
		Statute: Privacy Act of 1974 (P.L. 93-579);
		HHS: IS2P 2014;	

	OMB Memo: M-17-12, M-06-16;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AC-20(05)**	**Control Name** **Portable Storage Devices - Prohibited Use**	**Priority** **P2**	**CMS Baseline** **Above Baseline**
Control Statement Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.			
Discussion Limits on the use of organization-controlled portable storage devices in external systems include a complete prohibition of the use of such devices. Prohibiting such use is enforced using technical methods and/or nontechnical (i.e., process-based) methods.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls MP-7, PL-4, PS-6, SC-41.		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AC-21**	**Control Name** **Information Sharing**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**
Control Statement (a) Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for approved information-sharing circumstances where user discretion is required; and (b) Employ defined automated mechanisms, or manual processes (defined in applicable security and privacy plans) to assist users in making information sharing and collaboration decisions.			
Discussion Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	
Related Controls		**Reference Policy**	

AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15;	Code: 5 U.S.C. §552a(b), §552a(e);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.308(a)(4)(ii)(C), 45 C.F.R. §164.310(a)(2)(iii), 45 C.F.R. §164.310(b), 45 C.F.R. §164.312(a)(1), 45 C.F.R. §164.314(a);
	NISTIR: 8062;
	NIST SP: 800-150;
	OMB Circular: A-130;
	Privacy: Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment;

Privacy Discussion	
Privacy Implementation Standards Systems processing, storing, or transmitting PII (to include PHI): High & Moderate: PRIV.1 - PII may only be shared when authorized, there is a need to know, and adequate assurances of protection have been provided. (a) The sharing of PII must be in accordance with authorized government purposes. (b) Recipients of the shared information must have a need for the PII in the performance of their official duties. PRIV.2 - The sharing of PII, including PHI, must be in compliance with Privacy Act of 1974, E-Government Act of 2002 (Section 208), and HIPAA. PRIV.3 - Consistent with the Purpose Specification and Use Limitation Fair Information Practice Principles (FIPPs), sharing of PII must be compatible with the purpose for which it was collected. Consistent with the Transparency FIPP, any subsequent sharing that is not compatible may not be done until additional notice is provided to the individual, their consent is obtained, and relevant documents are updated or published; e.g., when applicable and appropriate, publish an updated system of records notice (SORN) to cover the additional incompatible sharing and obtain consent from the affected individuals.	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
AC-22	**Publicly Accessible Content**	**P3**	**Low** **Moderate** **High**
Control Statement (a) Designate individuals authorized to make information publicly accessible; (b) Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; (c) Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and (d) Review the content on the publicly accessible system for nonpublic information bi-weekly (no less often than 14 days) and remove such information, if discovered.			
Discussion In accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including information protected under the [PRIVACT] and proprietary information. Publicly accessible content addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Posting information on non-organizational systems (e.g., non-organizational public websites, forums, and social media) is covered by organizational policy. While organizations may have individuals who are responsible for developing and implementing policies about the information that can be made publicly accessible, publicly accessible content addresses the management of the individuals who make such information publicly accessible. This control addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. The posting of information on non-CMS systems is covered by organizational policy.			

Implementation Standard	
Control Review Frequency Bi-Weekly	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-3, AC-4, AT-2, AT-3, AU-13;
	Reference Policy
	Code: 5 U.S.C. §552(b)(6);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	HIPAA: 45 C.F.R. §164.502(a);
	OMB Memo: M-11-02;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Awareness and Training

Control Number	Control Name	Priority	CMS Baseline
AT-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel and roles:
   1. CMS Enterprise-level awareness and training policy that:
      a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

(c) Review and update the current awareness and training:
   1. Policy at least every three hundred sixty-five (365) days and following CMS-defined events (e.g. assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
   2. Procedures at least every three hundred sixty-five (365) days and following CMS-defined events (e.g. assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

Awareness and training policy and procedures address the controls in the AT family that are implemented within systems and at the CMS Enterprise-level. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of awareness and training policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to awareness and training policy and procedures include assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise-level awareness and training policy within the CMS IS2P2, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system-level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures).

Implementation Standard

High, Moderate & Low:

Std.1 - The CIO and CISO will provide leadership and oversight to:

(a) Develop, document, and disseminate to applicable personnel and roles:
   1. CMS Enterprise-level awareness and training policy that:
      a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

(c) Review and update the current awareness and training:
   1. Policy at least every three hundred sixty-five (365) days and following CMS-defined events (e.g. assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
   2. Procedures at least every three hundred sixty-five (365) days and following CMS-defined events (e.g. assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls PM-9, PS-8, SI-12; (Redacted Privacy Controls: AR-5, AR-6)	**Reference Policy** Code: 5 U.S.C. §552a(e)(9)-(10), Public Law (PL) No. 107-347, §208; Executive Order: 13587; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3, SM-4; HIPAA: 45 C.F.R. §164.308(a)(5)(i), 45 C.F.R. §164.308(a)(5)(ii)(A), 45 C.F.R. §164.308(a)(5)(ii)(B); NIST SP: 800-12, 800-16, 800-30, 800-39, 800-50, 800-100; OMB Memo: M-03-22, M-17-12; OMB A-130.
Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): Security awareness and training complements privacy awareness and training efforts, particularly when awareness and training efforts address topics where the two disciplines overlap, such as on topics related to use, confidentiality, access, integrity, and the protection of sensitive information. Coordination between the information security and privacy offices on the proper use and protections to be afforded to personally identifiable information (PII) within awareness and training policies addresses the purpose, roles and responsibilities surrounding PII compliance.	
Privacy Implementation Standards Systems processing, storing, or transmitting PII (to include PHI): High & Moderate: PRIV.1 - Ensure monitoring for changes to applicable privacy laws, regulations, and overarching policy affecting awareness and training policies is performed no less often than once every 365 days to ensure the CMS and Mission/Business/System awareness and training policies remain effective. PRIV.2 - Ensure awareness and training policies support privacy to the greatest extent feasible throughout the system's life cycle.	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AT-02**	**Control Name** **Literacy Training and Awareness**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement a. Provide security and privacy literacy training to CMS system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and within every three hundred sixty-five (365) days thereafter; and 2. When required by system changes or following CMS-defined events that include, but are not limited to assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; b. Employ the following techniques to increase the security and privacy awareness of system users, phishing emails and other defined techniques (defined in security and privacy plan). Security and privacy awareness training may be integrated with general Information Assurance training; c. Update literacy training and awareness content at least once every three hundred sixty-five (365) days and following CMS-defined events that include, but are not limited to assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and d. Incorporate lessons learned from internal or external security or privacy incidents into literacy training and awareness techniques.			
Discussion CMS provides basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users. CMS determines the content of literacy training and awareness based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and privacy as well as actions by users to maintain security and personal privacy and to respond to suspected incidents. The content addresses the need for operations security and the handling of personally identifiable information. Awareness techniques include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices from organizational officials, and conducting awareness events. Literacy training after the initial training described in AT-2a.1, is conducted at a minimum frequency consistent with applicable laws, directives, regulations, and policies. Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations; or a subset of topics from the initial			

training. Updating literacy training and awareness content on a regular basis helps to ensure the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Implementation Standard

High, Moderate & Low:

Std.1 - Develop and implement an information security and privacy education and awareness training program for all employees and individuals working on behalf of CMS who access, use, manage, or develop systems.

Std.2 - Address an individuals' responsibilities associated with sending sensitive information in email within the information security and privacy education and awareness training.

Std.3 - Provide Privacy awareness training before granting access to CMS systems and networks, and within every three hundred sixty-five (365) days thereafter, to all employees and contractors. Explain the importance of and the responsibility for safeguarding PII and ensuring privacy as established in federal legislation and OMB guidance.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Annually (365 Days)
Related Controls	**Reference Policy**

AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16;
(Redacted Privacy Controls: AR-5, AR-6)
	Code: 5 U.S.C. §552a(e)(9)-(10);
	Pub. L. No. 107-347, §208;
	Executive Order: 13587;
	FedRAMP Rev. 4 Baseline;
	FISCAM: AS-1, SM-4;
	HIPAA: 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 45 C.F.R. §164.308(a)(5)(ii);
	NIST SP: 800-50, 800-160-2, 800-181;
	OMB Memo: M-03-22, M-17-12;
	OMB A-130;
	ODNI CTF.

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Literacy training and awareness complements privacy awareness and training efforts, particularly when awareness and training efforts address topics where the two disciplines overlap, such as on topics related to use, confidentiality, access, integrity, and the protection of sensitive information.

Discussion for systems processing, storing, or transmitting PHI:

The following elements of security and privacy training are addressable under HIPAA. Security and Privacy Awareness Training should include:

(i) periodic security and privacy updates;
(ii) procedures for guarding against, detecting, and reporting malicious software;
(iii) procedures for monitoring log-in attempts and reporting discrepancies; and
(iv) procedures for creating, changing, and safeguarding passwords.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Amend control to provide security and privacy literacy training and awareness that includes:

1. Identification of the system(s) a user will access that collects, maintains, stores, uses, or discloses PII;
2. Training that is commensurate with the PII confidentiality impact level;

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
AT-02(01)	**Practical Exercises**		**HVA**

Control Statement

Provide practical exercises in literacy training that simulate events and incidents.

Discussion

Practical exercises include no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links.

Implementation Standard

High, Moderate & Low:
Std.1 - Provide practical exercises in literacy training that simulate events and incidents in a CMS test environment in accordance with NIST SP: 800-50.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years

Related Controls	Reference Policy
CA-2, CA-7, CP-4, IR-3;	OMB A-130, NIST SP: 800-50, 800-160-2, 800-181, ODNI CTF.

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

Provide practical exercises in literacy training that simulate events and incidents.

HVA Discussion

Practical Exercises may include, for example, simulated counterfeit detection, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, or malicious weblinks. Training may be regularly updated to reflect the most current, exigent cybersecurity threats posed to the HVA or the organization. Organizations may also update the minimum training requirements to operate the HVA, which may require the HVA owner or operator to complete the new training.

HVA Implementation Standard

Implement a cybersecurity user awareness and training program for HVA system owners and operators that includes practical exercises.
Std.1 - The organization should administer practical exercises to the HVA owner/operator prior to first use of the HVA, after a significant change to the HVA such that the prior exercises no longer reflect the risks and functions of the current HVA; and when exercises, training courses or requirements are updated.

Control Number	Control Name	Priority	CMS Baseline
AT-02(02)	**Insider Threat**	**P1**	**Low** **Moderate** **High**

Control Statement

Provide literacy training on recognizing and reporting potential indicators of insider threats, such as:
a. Inordinate, long-term job dissatisfaction,
b. Attempts to gain access to information not required for job performance,
c. Unexplained access to financial resources,
d. Bullying or sexual harassment of fellow employees,
e. Workplace violence, and
f. Other serious violations of organizational policies, procedures, directives, rules, or practices.

Discussion

Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices. Literacy training includes how to communicate the concerns of employees and management regarding potential

indicators of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role. For example, training for managers may be focused on changes in behavior of team members, while training for employees may be focused on more general observations.	
Implementation Standard High, Moderate & Low: Std.1 - Ensure awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls PM-12;	**Reference Policy** FedRAMP: Rev. 4 Baseline; OMB A-130, NIST SP: 800-50, 800-160-2, 800-181, ODNI CTF.
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AT-02(03)**	**Control Name** **Social Engineering and Mining**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**
Control Statement Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.			
Discussion Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Literacy training includes information on how to communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.			
Implementation Standard High, Moderate & Low: Std.1 - Ensure literacy training includes how to recognize and report, through appropriate CMS and defined channels (defined in applicable security/privacy plans), potential attempts to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	
Related Controls None;		**Reference Policy** See Control AT-2;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

<table>
<tr><td><b>Control Number</b>
AT-02(04)</td><td><b>Control Name</b>
Suspicious Communications and Anomalous System Behavior</td><td><b>Priority</b>
P2</td><td><b>CMS Baseline</b>
Above Baseline</td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using CMS-defined indicators of malicious code (defined in applicable security/privacy plans).</td></tr>
<tr><td colspan="4"><b>Discussion</b>
A well-trained workforce provides another organizational control that can be employed as part of a defense-in-depth strategy to protect against malicious code coming into organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email (e.g., receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender that appears to be from a known sponsor or contractor). Personnel are also trained on how to respond to suspicious email or web communications. For this process to work effectively, personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in systems can provide organizations with early warning for the presence of malicious code. Recognition of anomalous behavior by organizational personnel can supplement malicious code detection and protection tools and systems employed by organizations.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High, Moderate & Low:
Std.1 - Ensure awareness training includes how to recognize and report, through appropriate CMS and channels (defined in applicable security/privacy plans), potentially suspicious email or web communications(e.g., receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender but who appears to be from a known sponsor or contractor) and anomalous behaviors in systems.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Not Specified</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
None;</td><td colspan="2"><b>Reference Policy</b>
See Control AT-2;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
AT-02(05)</td><td><b>Control Name</b>
Advanced Persistent Threat</td><td><b>Priority</b>
P2</td><td><b>CMS Baseline</b>
Above Baseline</td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Provide literacy training on the advanced persistent threat.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
An effective way to detect advanced persistent threats (APT) and to preclude successful attacks is to provide specific literacy training for individuals. Threat literacy training includes educating individuals on the various ways that APTs can infiltrate the organization (e.g., through websites, emails, advertisement pop-ups, articles, and social engineering). Effective training includes techniques for recognizing suspicious emails, use of removable systems in non-secure settings, and the potential targeting of individuals at home.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High, Moderate & Low:
Std.1 - Provide literacy training on the advanced persistent threat as supported by NIST SP: 800-39.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Not Specified</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
None;</td><td colspan="2"><b>Reference Policy</b>
See Control AT-2;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

Control Number AT-02(06)	**Control Name** Cyber Threat Environment	**Priority** P3	**CMS Baseline** Above Baseline
Control Statement a. Provide literacy training on the cyber threat environment; and b. Reflect current cyber threat information in system operations.			
Discussion Since threats continue to change over time, threat literacy training by the organization is dynamic. Moreover, threat literacy training is not performed in isolation from the system operations that support organizational mission and business functions.			
Implementation Standard High, Moderate & Low: Std.1 - (a) Provide literacy training on the cyber threat environment; and (b) Reflect the current cyber threat information in CMS systems' operations.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls RA-3		**Reference Policy** See Control AT-2;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number AT-03	**Control Name** Role-Based Training	**Priority** P1	**CMS Baseline** Low Moderate High
Control Statement a. Provide role-based security and privacy training to personnel (both contractor and employee) with the following roles and responsibilities in accordance with HHS Memorandum detailing Requirements for Role-Based Training of Personnel with Significant Security Responsibilities (current version) (i.e., significant information security and privacy responsibilities) and (defined in applicable CMS security/privacy policies and plans): 1. Within sixty (60) days of entering security and privacy roles and responsibilities before authorizing access to the system, information, or performing assigned duties, and within every three hundred sixty-five (365) thereafter; and 2. When required by system changes; and b. Update role-based training at least once every three hundred sixty-five (365) days and following CMS-defined events that include, but are not limited to assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and c. Incorporate lessons learned from internal or external security or privacy incidents into role-based training.			
Discussion Organizations determine the content of training based on the assigned roles and responsibilities of individuals and the security and privacy requirements of CMS, and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties. Roles that may require role-based training include system owners; authorizing officials; system security officers; privacy officers; acquisition and procurement officials; enterprise architects; systems engineers; software developers; systems security and privacy engineers; system, network, and database administrators; personnel conducting configuration management activities; personnel performing verification and validation activities; auditors; personnel having access to system-level software; control assessors; personnel with contingency planning and incident response duties; personnel with privacy management responsibilities; and personnel having access to personally identifiable information. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of CMS's security and privacy programs. Role-based training also applies			

to contractors who provide services to federal agencies. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Updating role-based training on a regular basis helps to ensure that the content remains relevant and effective. Events that may precipitate an update to role-based training content include, but are not limited to, assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Implementation Standard

High, Moderate & Low:

Std.1 - Require personnel with significant information security and privacy roles and responsibilities to undergo appropriate information system security and privacy training prior to authorizing access to CMS networks, systems, and/or applications; when required by significant information system or system environment changes; and when an employee enters a new position that requires additional role-specific training and refresher training within every three hundred sixty-five (365) days thereafter.

Std.2 - The minimal role-based security and privacy training received over a 365-day cycle must meet or exceed Federal/Departmental minimum requirements as described in the CMS Information System Security and Privacy Policy (IS2P2) role-based training (RBT) policy.

Std.3 - Information Security and Privacy awareness and training may be provided by CMS, or via a non-CMS FISMA system, or received by means of CMS- or HHS- approved RBT courses, professional development, certificate programs, and/or traditional college credit courses.

Std.4 - All CMS employees and contractors with significant information security and privacy roles and responsibilities that have not completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their RBT requirement.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Annually (365 Days)

Related Controls	**Reference Policy**

AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, IR-9, PL-4, PM-13, PM-23, PS-7, PS-9, SA-3, SA-8, SA-11, SA-16, SR-5, SR-6, SR-11;
(Redacted Privacy Controls: AR-5, AR-6)
	Code: 5 U.S.C. §552a(e)(9)-(10), Pub. L. No. 107-347, §208;
	FedRAMP Rev. 4 Baseline;
	FISCAM: AS-1, SM-4;
	HHS Memorandum: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities;
	HIPAA: 45 C.F.R. §164.308(a)(5)(i);
	45 C.F.R. §164.530(b)(2)(i);
	NIST SP: 800-16, 800-50, 800-181;
	OMB Memo: M-03-22, M-17-12;
	OMB A-130

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Significant information security and privacy responsibilities are defined as the responsibilities associated with a given role or position, which, upon execution, could have the potential to adversely impact the security and/or privacy posture of one or more CMS systems.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Amend control to provide role-based security and privacy training for all systems that collect, maintain, store, use, or disclose PII is commensurate with the PII confidentiality impact level.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
AT-03(01)	**Environmental Controls**		**Above Baseline**

Control Statement

Provide CMS-defined personnel (defined in system security and privacy plan) with initial and annual training in the employment and operation of environmental controls.

Discussion

Environmental controls include fire suppression and detection devices or systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature or humidity, heating ventilation, air conditioning, and power within the facility.

Implementation Standard	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls PE-1, PE-11, PE-13, PE-14, PE-15	**Reference Policy** See Control AT-3;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AT-03(02)**	**Control Name** **Physical Security Controls**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Provide all CMS personnel (employees and contractors) with initial and annual training in the employment and operation of physical security controls.			
Discussion Physical security controls include physical access control devices, physical intrusion and detection alarms, operating procedures for facility security guards, and monitoring or surveillance equipment.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls PE-2, PE-3, PE-4		**Reference Policy** See Control AT-3;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AT-03(03)**	**Control Name** **Practical Exercises**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Provide practical exercises in security and privacy training that reinforce training objectives.			
Discussion Practical exercises for security include training for software developers that addresses simulated attacks that exploit common software vulnerabilities or spear or whale phishing attacks targeted at senior leaders or executives. Practical exercises for privacy include modules with quizzes on identifying and processing personally identifiable information in various scenarios or scenarios on conducting privacy impact assessments.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None;		**Reference Policy** See Control AT-3;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AT-03(05)**	**Control Name** **Processing Personally Identifiable Information**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement

Provide to all CMS personnel (both contractor and employee) with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls.

Discussion

Personally identifiable information processing and transparency controls include the organization's authority to process personally identifiable information and personally identifiable information processing purposes. Role-based training for federal agencies addresses the types of information that may constitute personally identifiable information and the risks, considerations, and obligations associated with its processing. Such training also considers the authority to process personally identifiable information documented in privacy policies and notices, system of records notices, computer matching agreements and notices, privacy impact assessments, [PRIVACT] statements, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

Implementation Standard

High, Moderate & Low:

Std.1 – Develop and implement a privacy education and awareness training program for all employees and individuals working on behalf of CMS involved in managing, using, and/or processing PII.

Std.2 - Include responsibilities associated with sending PII in email within the privacy education and awareness training.

Std.3 - Ensure communications and training related to privacy and security is job-specific and commensurate with the employee's responsibilities.

Std.4 - Ensure the initial training of employees (including managers) on their privacy and security responsibilities is completed before permitting access to CMS information and systems. Thereafter, ensure refresher training is completed annually to ensure employees continue to understand their responsibilities.

Std.5 - Ensure provided additional or advanced training is commensurate with increased responsibilities or change in duties.

Std.6 - Include acceptable rules of behavior and the consequences when the rules are not followed within both initial and refresher training.

Std.7 - Ensure training addresses the rules for telework and other authorized remote access programs.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
PT-2, PT-3, PT-5, PT-6
	Reference Policy
	Code: 5 U.S.C. §552a(e)(9), 44 U.S.C.: §3541;
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) Title III §208, Telework Enhancement Act of 2010;
	HIPAA: 45 C.F.R. §164.530(b)(1), 45 C.F.R. §164.530(a)(1)(ii);
	HHS: IRM Policy for IT Security for Remote Access, Master Labor Agreement;
	NIST SP: 800-50, 800-181;
	OMB Circular: A-130;
	OMB Memo: M-03-22, M-05-08, M-06-16, M-17-12 Att. 1 and A.2.d.;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **AT-04**	**Control Name** **Training Records**	**Priority** **P3**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement

a. Identify employees and contractors who hold roles with significant information security and privacy responsibilities;

b. Document and monitors information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and
c. Retain individual training records for a minimum of five (5) years after completing a specific training course.

Discussion

Procedures and training implementation should:
a. Identify employees with significant information security and privacy responsibilities and provide role-specific training in accordance with NIST standards and guidance:
1. All users of CMS systems must be exposed to security and privacy awareness materials at least every 365 days. Users of CMS systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS systems and applications;
2. Executives must receive training in information security and privacy basics and policy level training in security and privacy planning and management;
3. Program and functional managers must receive training in information security and privacy basics; management and implementation level training in security and privacy planning and system/application security and privacy management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning;
4. CIOs, information security and privacy program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security and privacy officers) must receive training in information security and privacy basics and broad training in security and privacy planning, system and application security and privacy management, system/application life cycle management, risk management, and contingency planning; and
5. IT function management and operations personnel must receive training in information security and privacy basics; management and implementation level training in security and privacy planning and system/application security and privacy management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.
b. CMS must provide the CMS systems security awareness material/exposure outlined in NIST guidance on information security awareness and training to all new employees before allowing them access to the systems;
c. CMS must provide system security and privacy refresher training for employees as frequently as CMS determines necessary, based on the sensitivity of the information that the employees use or process; and
d. CMS must provide training whenever there is a significant change in the system environment or procedures or when an employee enters a new position that requires additional role-specific training.
e. Documentation for specialized training may be maintained by individual supervisors at the discretion of the organization. The National Archives and Records Administration provides guidance on records retention for federal agencies.

Implementation Standard

High, Moderate & Low:
Std.1 - (a) Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and
(b) Retain individual training records for a minimum of five (5) years after completing a specific training course.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Annually (365 Days)

Related Controls	**Reference Policy**

AT-2, AT-3, CP-3, IR-2, PM-14, SI-12;
(Redacted Privacy Controls: AR-5, AR-6)
	Code: 5 U.S.C. §552a(e)(9)-(10), Pub. L. No. 107-347, §208;
	FedRAMP Rev. 4 Baseline;
	FISCAM: AS-1, SM-4;
	HIPAA: 45 C.F.R. §164.308(a)(5)(i);
	45 C.F.R. §164.308(a)(5)(i); 45 C.F.R. §164.530(b)(2)(ii) HHS Memorandum: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities
	OMB Memo: M-03-22, M-17-12;
	OMB A-130.

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
Maintaining security and privacy training records provides the capability for CMS and CMS Businesses/Systems to track compliance with privacy-related training requirements. Under HIPAA, a covered entity must document that the training as described within the regulation has been provided as required.

Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Audit and Accountability

Control Number **AU-01**	**Control Name** **Policy and Procedures**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel or roles:

1. CMS Enterprise-level, audit and accountability policy that:
   a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

(c). Review and update the current audit and accountability:

1. Policy at least every three (3) years and following CMS-defined events (e.g. assessment or audit findings, security or privacy incidents, changes in laws, executive orders, etc.);and
2. Procedures at least every three (3) years and following CMS-defined events (e.g. assessment or audit findings, security or privacy incidents, changes in laws, executive orders, etc.).

Discussion

Audit and accountability policy and procedures address the controls in the AU family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of audit and accountability policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to audit and accountability policy and procedures include assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise level audit and accountability policy within the CMS IS2P2, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures.)

Implementation Standard

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
PM-9, PS-8, SI-12.
(Redacted Privacy Controls: AR-4)
	Reference Policy
	FedRAMP Rev. 4 Baseline;
	FISCAM: AS-1, SM-1, SM-3;
	HIPAA: 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D);
	NIST SP: 800-12, 800-100,800-30, 800-39;
	OMB M-17-12, Circular A-130, 7.g., and 8.b(2)(c)

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion
HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
AU-02	**Event Logging**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

(a). Identify, based on a risk assessment and CMS mission/business needs, the types of events specified in Implementation Standard 1 that the system is capable of logging in support of the audit function;
(b). Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
(c).Specify the following event types in Implementation Standard 2 require logging on a continuous basis within the system;
(d). Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
(e). Review and update the event types selected for logging no less often than every three hundred sixty-five (365) days and whenever there is a significant system modification.

Discussion

An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, organizations consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.

To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. The types of events that organizations desire to be logged may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization. Organizations consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the logging event is based on patterns or time of usage.

Event logging requirements, including the need to log specific event types, may be referenced in other controls and control enhancements. These include AC-2(4), AC-3(10), AC-6(9), AC-17(1), CM-3f, CM-5(1), IA-3(3.b), MA-4(1), MP-4(2), PE-3, PM-21, PT-7, RA-8, SC-7(9), SC-7(15), SI-3(8), SI-4(22), SI-7(8), and SI-10(1). Organizations include event types that are required by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of event logging is an important part of a monitoring and auditing capability and can identify the root causes of problems. When defining event types, organizations consider the logging necessary to cover related event types, such as the steps in distributed, transaction-based processes and the actions that occur in service-oriented architectures.

Implementation Standard

High & Moderate:
Std.1 - List of auditable events:
(a) Server alerts and error messages;
(b) User log-on and log-off (successful or unsuccessful);
(c) All system administration activities;
(d) Modification of privileges and access;
(e) Start up and shut down;
(f) Application modifications;
(g) Application alerts and error messages;
(h) Configuration changes;
(i) Account creation, modification, or deletion;

(j) File creation and deletion;
(k) Read access to sensitive information;
(l) Modification to sensitive information;
(m) Printing sensitive information;
(n) Anomalous (e.g., non-attributable) activity;
(o) Data as required for privacy monitoring privacy controls;
(p) Concurrent log on from different work stations;
(q) Override of access control mechanisms; and
(r) Process creation.
Std.2 - Subset of Implementation Standard 1 auditable events:
(a) User log-on and log-off (successful or unsuccessful);
(b) Configuration changes;
(c) Application alerts and error messages;
(d) All system administration activities;
(e) Modification of privileges and access;
(f) Account creation, modification, or deletion;
(g) Concurrent log on from different work stations; and
(h) Override of access control mechanisms.
Std.3 - Verify that proper logging is enabled to audit administrator activities.
Std.4 - Information collected will be compliant with the Federal Rules of Evidence.
Std. 5 - The organization reviews and updates the list of auditable events at least every three hundred sixty-five (365) days and whenever there is a change in the threat environment
Low:
Std.1 - List of auditable events:
(a) Server alerts and error messages;
(b) User log-on and log-off (successful or unsuccessful);
(c) All system administration activities;
(d) Modification of privileges and access;
(e) Start up and shut down;
(f) Application modifications;
(g) Application alerts and error messages;
(h) Configuration changes;
(i) Account creation, modification, or deletion;
(j) File creation and deletion;
(k) Read access to sensitive information;
(l) Modification to sensitive information;
(m) Anomalous (e.g., non-attributable) activity;
(n) Concurrent log on from different work stations;
(o) Override of access control mechanisms; and
(p) Process creation.
Std.2 - Subset of Implementation Standard 1 auditable events:
(a) User log-on and log-off (successful or unsuccessful);
(b) Configuration changes;
(c) Application alerts and error messages;
(d) All system administration activities;
(e) Modification of privileges and access;

(f) Account creation, modification, or deletion;
(g) Concurrent log on from different work stations; and
(h) Override of access control mechanisms.
Std.3 - Verify that proper logging is enabled to audit administrator activities.
Std.4 - Information collected will be compliant with the Federal Rules of Evidence.

Control Review Frequency Weekly	**Assessment Frequency** Three (3) Years

Related Controls
AC-2, AC-3,AC-6, AC-7, AC-8, AC-16,AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-2, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC-7, SC-18, SI-3, SI-4,SI-7, SI-10, SI-11.
(Redacted Privacy Controls: AR-4)
	Reference Policy
	FedRAMP Rev. 4 Baseline;
	FISCAM: AC-5, AS-2;
	HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(C), 45 C.F.R. §164.312(b), 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R; NIST SP: 800-37, 800-39, 800-92, 800-137;
	OMB Memo: M-14-03, M-15-01, M-16-04, M-06-16, M-17-12;
	OMB Circular A-130, 7.g., 8.b(2)(c)(iii) and Appendix I; Web:csrc.nist.gov/pcig/cig.html

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a). Identify, based on a risk assessment and CMS mission/business needs, the types of events specified in Implementation Standard 1 that the system is capable of logging in support of the audit function;
(b). Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
(c). Identify and specify, based on a risk assessment and CMS mission/business needs, the following types of events require auditing and logging on a continuous basis for HVAs:

1. Audit success and failed logons (OS and data repositories);
2. Audit success and failed computer account activities (OS and data repositories);
3. Audit success and failed account and user management activities (OS and data repositories);
4. Unsuccessful attempts to access database;
5. Enterprise synchronized date, time, and time zone for each event;
6. Source IP, port and protocol;
7. Destination IP, port and protocol;

(d). Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
(e). Review and update the event types selected for logging no less often than every three hundred sixty-five (365) days and whenever there is a significant system modification.

HVA Discussion

Given the sensitivity of the information and systems, the analysis of the logs and events are performed more frequently and with more rigor than non-HVA systems. Reporting of potential incidents comply with US-CERT requirements. Cyber-relevant time is the relative speed at which an adversary is attacking a network, application, system, or other resource

HVA Implementation Standard

Audit successful and failed logins (Operating System [OS] and data repositories), audit success and failed computer account activities (OS and data repositories), audit success and failed account and user management activities (OS and data repositories), unsuccessful attempts to access database, enterprise synchronized date, time, and time zone for each event, source Internet Protocol (IP), port and protocol, destination IP, port and protocol, and others.

Control Number **AU-03**	**Control Name** **Content of Audit Records**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

Discussion

Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f) . Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

Implementation Standard

Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)
Related Controls AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7,SI-11 (Redacted Privacy Controls: AR-4)	**Reference Policy** FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); OMB Memo: M-06-16, M-17-12 Att. 1 OMB Circular A-130: 7.g., and 8.b(2)(c)(iii); IR 8062

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **AU-03(01)**	**Control Name** **Additional Audit Information**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement

Generate audit records containing the following additional information and event details explicitly needed for audit requirements. At a minimum, the audit records must contain the following:
- Filename accessed;
- Program or privileged commands used to initiate the event; and
- Source and destination addresses; and

Discussion

The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records including, but not limited to, access control or flow control rules invoked and individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. This facilitates the use of audit trails and audit logs by not including information in audit records that could potentially be misleading, make it more difficult to locate information of interest, or increase the risk to individuals' privacy.	
Implementation Standard	
Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)
Related Controls	**Reference Policy** FedRAMP Rev. 4 Baseline
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
AU-03(03)	**Limit Personally Identifiable Information Elements**		**Moderate** **High**

Control Statement Limit personally identifiable information contained in audit records to the defined elements identified in the privacy risk assessment (Note: Identify the System defined elements in the PIA. E.g. Social Security Number)	
Discussion Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.	
Implementation Standard Std 1. Identify the minimum PII elements that are relevant and necessary to accomplish the purpose of collection (and where a collection of certain PII requires legal authorization, HHS/CMS must ensure that such collection is legally authorized);	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls RA-3	**Reference Policy**
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
AU-04	**Audit Log Storage Capacity**	**P1**	**Low** **Moderate** **High**

Control Statement Allocate audit log storage capacity to accommodate and configure auditing to reduce the likelihood of such capacity being exceeded as specified in Implementation Standard 1.
Discussion

Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.	
Implementation Standard High, Moderate & Low: Std.1 - Capacity must be sufficient to handle auditing records during peak performance times (e.g., open enrollment).	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14,SI-4
(Redacted Privacy Controls: AR-4)
	Reference Policy
	Code: 5 U.S.C. §552a(i);
	FedRAMP Rev. 4 Baseline;
	FISCAM: AC-5, AS-2;
	HIPAA: 164.312(b);
	OMB Memo: M-17-12;
	OMB Circular A-130: 7.g. and Appendix II; 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D)

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
AU-05	**Response to Audit Logging Processing Failures**	**P1**	**Low** **Moderate** **High**
Control Statement (a). Alert defined personnel or roles (e.g., System Administrator and ISSO)[defined in the applicable system security and privacy plan] in the event of an audit logging process failure as specified in Implementation Standard 1; and (b). Take the actions defined in Implementation Standard 1in response to an audit failure or audit storage capacity issue.			
Discussion Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization-defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored),the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.			
Implementation Standard High & Moderate: Std.1 - Takes the following actions in response to an audit failure or audit storage capacity issue: (a) Shutdown the information system or halt processing immediately; and (b) Systems that do not support automatic shutdown must be shut down within 1 hour of the audit processing failure. Low: Std.1 - Takes the following actions in response to an audit failure or audit storage capacity issue: (a) Shutdown the information system or halt processing; (b) Stop generating audit records; or (c) Overwrite the oldest records, in the case that storage media is unavailable.			

<table>
<tr><td><b>Control Review Frequency</b>
Quarterly</td><td><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td><b>Related Controls</b>
AU-2, AU-4,AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12</td><td><b>Reference Policy</b>
FedRAMP Rev. 4 Baseline;
FISCAM: AC-5, AS-2</td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="2"><b>HVA Discussion</b></td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>AU-05(01)</b></td><td><b>Control Name</b>
<b>Storage Capacity Warning</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Provide a warning to defined personnel or roles, and/or locations (e.g., System Administrator and ISSO)[defined in the applicable system security and privacy plan] within a defined time period (defined in the applicable system security and privacy plan)when allocated audit log storage volume reaches 80% of repository maximum audit log storage capacity.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Organizations may have multiple audit log storage repositories distributed across multiple system components with each repository having different storage volume capacities.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b></td><td colspan="2"><b>Reference Policy</b></td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>AU-05(02)</b></td><td><b>Control Name</b>
<b>Real-Time Alerts</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Provide an alert in real-time to defined personnel or roles and/or locations (e.g., System Administrator and ISSO)[defined in the applicable system security and privacy plan] when the following audit failure events occur:
- Record log is full;
- Auditing application reports an error;
- Authentication logging failure; and
- Encryption logging failure.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Monthly</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
</table>

Related Controls	**Reference Policy**
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
AU-06	**Audit Record Review, Analysis, and Reporting**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

(a). Review and analyze system audit records no less often than weekly [seven (7) days] for indications of inappropriate or unusual activity as defined within the Implementation Standards and the potential impact of the inappropriate or unusual activity;
(b). Report findings to defined personnel or roles (defined in the applicable system security and privacy plan);and
(c). Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Discussion

Audit record review, analysis, and reporting covers information security- and privacy-related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The frequency, scope, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

Implementation Standard

High:
Std.1 - Review system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resource utilization to determine anomalies no less often than once within a twenty-four (24) hour period and on demand. Generate alert notification for technical personnel review and assessment.
Std.2 - Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies no less often than once within a twenty- four (24) hour period and on demand. Generate alerts for technical personnel review and assessment.
Std.3 - Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.
Std.4 - Use automated utilities to review audit records no less often than once every twenty-four (24) hours for unusual, unexpected, or suspicious behavior.
Std.5 - Inspect administrator groups on demand but no less often than once every seven (7) days to ensure unauthorized administrator, system, and privileged application accounts have not been created.
Std.6 - Perform manual reviews of system audit records randomly on demand but no less often than once every thirty (30) days.
Moderate:
Std.1 - Review system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resource utilization to determine anomalies no less often than once within a twenty-four (24) hour period and on demand. Generate alert notification for technical personnel review and assessment.
Std.2 - Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies no less often than once within a twenty- four (24) hour period and on demand. Generate alerts for technical personnel review and assessment.
Std.3 - Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.

Std.4 - Use automated utilities to review audit records no less often than once every seventy-two (72) hours for unusual, unexpected, or suspicious behavior. Std.5 - Inspect administrator groups on demand but no less often than once every fourteen (14) days to ensure unauthorized administrator, system, and privileged application accounts have not been created.

Std.6 - Perform manual reviews of system audit records randomly on demand but no less often than once every thirty (30) days.

Low:

Std.1 - Review system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resource utilization to determine anomalies no less often than once within a twenty-four (24) hour period and on demand. Generate alert notification for technical personnel review and assessment.

Std.2 - Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies no less often than once within a twenty- four (24) hour period and on demand. Generate alerts for technical personnel review and assessment.

Std.3 - Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.

Std.4 - Use automated utilities to review audit records no less often than every seventy-two (72) hours for unusual, unexpected, or suspicious behavior.

Std.5 - Inspect administrator groups on demand but no less often than once every thirty (30) days to ensure unauthorized administrator, system, and privileged application accounts have not been created.

Std.6 - Inspect administrator groups on demand but no less often than once every thirty (30) days to ensure unauthorized administrator accounts have not been created.

Control Review Frequency Weekly	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2,CA-7, CM-2,CM-5, CM-6,CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7
(Redacted Privacy Controls: AR-4)
	Reference Policy
	Code: 5 U.S.C. §552a(g)(1)(D);
	FedRAMP Rev. 4 Baseline;
	FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(5)(ii)(C), 45 C.F.R. §164.312(b);
	NIST SP: 800-37, 800-39, 800-115, 800-137;
	OMB Memo: M-7-16, M-14-03, M-15-01, M-16-04

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a). Review, analyze, and alert HVA systems audit records in real-time for indications of inappropriate, unusual activity (i.e., concurrent logons), breaches, or threats;

(b). Report incidents and findings to defined personnel or roles (defined in the applicable system security and privacy plan) and in accordance with US-CERT reporting timeframes and requirements; and

(c). Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

HVA Discussion

Given the sensitivity of the information and systems, the analysis of the logs and events are performed more frequently and with more rigor than non-HVA systems. Reporting of potential incidents comply with US-CERT requirements. Cyber-relevant time is the relative speed at which an adversary is attacking a network, application, system, or other resource

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
AU-06(01)	**Automated Process Integration**	**P1**	**Moderate** **High**

Control Statement

<table>
<tr><td colspan="2">Integrate audit record review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities using automated mechanisms (defined in applicable system security and privacy plan).</td></tr>
<tr><td colspan="2"><b>Discussion</b>
Organizational processes that benefit from integrated audit record review, analysis, and reporting include incident response, continuous monitoring, contingency planning, investigation and response to suspicious activities, and Inspector General audits.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.</td></tr>
<tr><td colspan="2"><b>Implementation Standard</b>
High & Moderate:
Std.1 - Aggregated audit records from automated information security capabilities and service tools must be searchable by the CCIC:
(a)Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b)Audit records sources include systems, appliances, devices, services, and applications (including databases).
(c)CCIC directed audit information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw audit records must be available in an unaltered format to the CCIC.
Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.</td></tr>
<tr><td><b>Control Review Frequency</b>
Monthly</td><td><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td><b>Related Controls</b>
PM-7</td><td><b>Reference Policy</b>
FedRAMP Rev. 4 Baseline;
NIST SP: 800-115, 800-137;
OMB Memo: M-14-03, M-15-01, M-16-04</td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="2"><b>HVA Discussion</b></td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>AU-06(03)</b></td><td><b>Control Name</b>
<b>Correlate Audit Record Repositories</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Moderate</b>
<b>High</b>
<b>HVA</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and supports cross-organization awareness.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High & Moderate:
Std.1 - Correlated results from automated tools must be searchable by the CCIC:
(a)Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b)Repository sources include systems, appliances, devices, services, and applications (including databases); and
(c)CCIC directed repository information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw audit records must be available in an unaltered format to the CCIC.</td></tr>
</table>

Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.	
Control Review Frequency Quarterly	**Assessment Frequency** Three (3) Years

Related Controls
AU-12, IR-4
	Reference Policy
	Code: 5 U.S.C. §552a(g)(1)(D);
	FedRAMP Rev. 4 Baseline;
	OMB Memo: M-7-16

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Analyze and correlate audit records across different repositories to gain organization-wide situational awareness and form a single risk view of the enterprise.	
HVA Discussion Audit data collected at the system level (Tier 3) should be aggregated with audit data from other systems to form a system-level enterprise view of audit records. Audit information must be protected at a level congruent with the highest level of information it contains (AU-9). Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and support cross-organization awareness. Organization-wide situational awareness includes awareness across all three levels of risk management and support cross-organization awareness.	
HVA Implementation Standard Manage enterprise risk by correlating audit logs and events from all organizational systems to form a single risk view of the enterprise.	

Control Number **AU-06(05)**	**Control Name** **Integrated Analysis of Audit Records**	**Priority** **P1**	**CMS Baseline** **High** **HVA**
Control Statement Integrate analysis of audit records with analysis of (one or more of the following, defined in the applicable system security and privacy plan): vulnerability scanning information; performance data; system monitoring information; and/or other defined data/information collected from other sources (defined in the applicable system security and privacy plan) to further enhance the ability to identify inappropriate or unusual activity.			
Discussion Integrated analysis of audit records does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, integrated analysis requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. Security Information and Event Management tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans of the system and in correlating attack detection events with scanning results. Correlation with performance data can uncover denial-of-service attacks or other types of attacks that result in the unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations. Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.			
Implementation Standard High: Std.1 - Aggregated vulnerability scanning information, performance data, and network monitoring information from automated tools must be searchable by the CCIC: (a)Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; (b)Information sources include systems, appliances, devices, services, and applications (including databases); and (c)CCIC directed information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.2 - As required by CMS, raw vulnerability scanning information, performance data, and network monitoring information must be available in an unaltered format to the CCIC. Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.			

Control Review Frequency Quarterly	**Assessment Frequency** Three (3) Years
Related Controls AU-12, IR-4, RA-5	**Reference Policy** NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Integrate analysis of audit records with analysis of (one or more of the following, defined in the applicable system security and privacy plan): vulnerability scanning information; performance data; system monitoring information; and/or other defined data/information collected from other sources (defined in the applicable system security and privacy plan) to further enhance the ability to identify inappropriate or unusual activity.	
HVA Discussion Integrated analysis of audit records does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, integrated analysis requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. Security Information and Event Management tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans of the system and in correlating attack detection events with scanning results. Correlation with performance data can uncover denial of service attacks or other types of attacks resulting in unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.	
HVA Implementation Standard Identify threats, inappropriate actions, or unusual activities by correlating audit record information with vulnerability, performance data, and/or system monitoring information.	

Control Number **AU-06(06)**	**Control Name** **Correlation with Physical Monitoring**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.			
Discussion The correlation of physical audit record information and the audit records from systems may assist organizations in identifying suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identity for logical access to certain systems with the additional physical security information that the individual was present at the facility when the logical access occurred may be useful in investigations.			
Implementation Standard			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	
Related Controls		**Reference Policy** NIST SP: 800-100, 800-61	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number	Control Name	Priority	CMS Baseline
AU-07	**Audit Record Reduction and Report Generation**	**P2**	**Moderate** **High**

Control Statement

Provide and implement an audit record reduction and report generation capability that:
(a). Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and
(b). Does not alter the original content or time ordering of audit records.

Discussion

Audit record reduction is a process that manipulates collected audit log information and organizes it into a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities that conduct audit logging activities. The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be an issue if the granularity of the timestamp in the record is insufficient.
Event collection and analysis software can perform event reduction by disregarding data that are not significant to information system security, potentially increasing its efficiency in network and storage resource needs.

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)

Related Controls	Reference Policy

AC-2, AU-2, AU-3, AU-4, AU-5, AU-6,AU-12, AU-16, CM-5, IA-5, IR-4, PM-12, SI-4	FedRAMP Rev. 4 Baseline;
	FISCAM: AC-5, AS-2;
	HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.312(b);
	NIST SP: 800-137;
	OMB Memo: M-17-12, Att. 2

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
AU-07(01)	**Automatic Processing**	**P2**	**Moderate** **High**

Control Statement

Provide and implement the capability to process, sort, and search audit records for events of interest based on selectable event criteria and defined fields within audit records (defined in applicable system security and privacy plan).

Discussion

Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure. Organizations may define event criteria to any degree of granularity required, such as locations selectable by a general networking location or by specific system component.
Sorting and searching of audit records may be based upon the contents of audit record fields, for example: (i) date/time of events; (ii) user identifiers; (iii) Internet Protocol (IP) addresses involved in the event; (iv) type of event; or (v) event success/failure.

Implementation Standard

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls	**Reference Policy**
	FedRAMP Rev. 4 Baseline;
	OMB Memo: M-17-12, Att. 2;
	HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b)

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AU-08**	**Control Name** **Time Stamps**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement

(a). Use internal system clocks to generate time stamps for audit records; and

(b). Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and is accurate to within one hundred (100) milliseconds.

Discussion

Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds of milliseconds or tens of milliseconds). Organizations may define different time granularities for different system components. Time service can be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns. The consistent log timestamps facilitate effective event correlation.

Implementation Standard

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls AU-3, AU-12,AU-14, SC-45.	**Reference Policy** FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
AU-09	**Protection of Audit Information**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

(a). Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

(b). Alert defined personnel or roles (e.g., System Administrator and ISSO) (defined in the applicable system security and privacy plan)upon detection of unauthorized access, modification, or deletion of audit information.

Discussion

Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.

Implementation Standard

High:

Std.1 - Cryptographic mechanisms shall be employed to protect the integrity of audit information (e.g. log, and audit tools).

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)

Related Controls	Reference Policy

AC-3, AC-6, AU-6, AU-11, AU-14, AU-15,MP- 2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4.	Code: 5 U.S.C. §552a(i);
	FedRAMP Rev. 4 Baseline;
	FISCAM: AC-5, AS-2;
	OMB Memo: M-17-12;
	OMB Circular A-130: 7.g. and Appendix II;
	HIPPA: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b);
	FIPS: 140-3, 180-4, 202

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a). Protect audit information and audit logging tools from unauthorized access, modification, and deletion to the highest level commensurate with the security protection level of the information contained within the audit events;

(b). Alert defined personnel or roles (e.g., System Administrator and ISSO) [defined in the applicable system security and privacy plan] upon detection of unauthorized access, modification, or deletion of audit information.

HVA Discussion

Audit information includes all information, for example, audit records, audit log settings, audit reports, and personally identifiable information, needed to successfully audit system activity. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls

HVA Implementation Standard

Ensure audit information is protected to the highest level commensurate with the highest security protection level of the information contained within the audit events.

Control Number **AU-09(02)**	Control Name **Store on Separate Physical Systems or Components**	Priority **P1**	CMS Baseline **High** **HVA**
Control Statement Store audit records no less often than weekly [seven (7) days] in a repository that is part of a physically different system or system component than the system or component being audited.			
Discussion Storing audit records in a repository separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organization-wide activity. Storing audit records on separate systems or components applies to initial generation as well as backup or long-term storage of audit records.			
Implementation Standard High: Std.1 - The centralized audit servers must meet this control. Std.2 - The centralized audit server must be separated from the audit client information systems.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
AU-4, AU-5
		Reference Policy
		FedRAMP Rev. 4 Baseline;
		NIST SP: 800-137;
		FIPS: 140-3, 180-4, 202	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement (a). Store audit records no less often than weekly [seven (7) days] in a repository that is part of a physically different system or system component of the highest sensitivity level commensurate with the security protection level as the HVA system being audited.			
HVA Discussion Storing audit records in a repository separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organization-wide activity. Storing audit records on separate systems or components applies to initial generation as well as backup or long-term storage of audit records.			
HVA Implementation Standard Protect system audit information by storing/transferring audit information to a physically different system from the system that generated the events.			

Control Number **AU-09(03)**	Control Name **Cryptographic Protection**	Priority **P1**	CMS Baseline **High** **HVA**
Control Statement Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.			
Discussion Cryptographic mechanisms used for protecting the integrity of audit information include signed hash functions using asymmetric cryptography. This enables the distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	

Related Controls
AU-10, SC-12, SC-13
		Reference Policy
		Code: 5 U.S.C. §552a(i);
		OMB Circular A-130: 7.g. and Appendix II;	

	45 C.F.R. §164.306(a)(1); 45 C.F.R. §164.312(a)(2)(iv); FIPS: 140-3, 180-4, 202
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Implement cryptographic mechanisms (e.g., hashing function) to protect the integrity of audit information and audit tools.	
HVA Discussion Cryptographic mechanisms used for protecting the integrity of audit information include signed hash functions using asymmetric cryptography. This enables the distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.	
HVA Implementation Standard	

Control Number **AU-09(04)**	**Control Name** **Access by Subset of Privileged Users**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Authorize access to management of audit logging functionality to only individuals or roles who are not subject to audit by that system (defined in applicable system security and privacy plan).			
Discussion Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.			
Implementation Standard			
Control Review Frequency Quarterly		**Assessment Frequency** Three (3) Years	

Related Controls
AC-5
(Redacted Privacy Controls: AR-5)
		Reference Policy
		Code: 5 U.S.C. §552a(b)(1);
		FedRAMP Rev. 4 Baseline;
		FIPS: 140-3, 180-4, 202	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AU-09(05)**	**Control Name** **Dual Authorization**	**Priority**	**CMS Baseline** **HVA**
Control Statement Enforce dual authorization for movement and deletion of system audit information by CMS-defined officials (e.g., CMS Senior Management such as the AO, CISO, SOP) and [CMS Entity-Defined: Mission/Business process-level/System-level]-defined officials (e.g., Business Owner, System Owner, ISSO).			
Discussion Organizations may choose different selection options for different types of audit information. Dual authorization mechanisms (also known as two-person control) require the approval of two authorized individuals to execute audit functions. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. Organizations do not require dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.			
Implementation Standard			
Control Review Frequency		**Assessment Frequency**	

Annually (365 Days)	Three (3) Years
Related Controls AC-3.	**Reference Policy**
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Enforce dual authorization, two appropriate organizational personnel such as CMS-defined officials (e.g., CMS Senior Management such as the AO, CISO, SOP) and [CMS Entity-Defined: Mission/Business process-level/System-level]-defined officials (e.g., Business Owner, System Owner, ISSO) for manual movement and deletion of HVA systems audit logs and information.	
HVA Discussion To protect the integrity and availability of audit information organizations control access and authorizations of privileged users to modify and delete audit logs. Logs are retained in accordance with federal, department, and agency requirements. After the retention requirement period organizations may have a need to delete or move audit information from systems. Dual authorization approvals by at least two appropriate personnel (system owner, mission/business owner, AO, CISO, etc.) is required for movement or deletion of audit files. Automated systems can be configured to automatically archive or remove audit logs according to policy.	
HVA Implementation Standard	

Control Number **AU-09(06)**	**Control Name** **Read Only Access**	**Priority**	**CMS Baseline** **HVA**
Control Statement Authorize read-only access to audit information to authorized individuals or roles (defined in applicable system security and privacy plan) subset of privileged users or roles.			
Discussion Restricting privileged user or role authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users or roles, such as deleting audit records to cover up malicious activity.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	
Related Controls		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Authorize read-only access to audit information to authorized individuals or roles (defined in applicable system security and privacy plan) with privileged accounts only.			
HVA Discussion Only limited privilege accounts with the need to know have read-only access to audit logs. All other users do not have any access to HVA logs. Organizations limit and restrict any accounts, in accordance with AU-9(5), with access to write or delete audit logs.			
HVA Implementation Standard Ensure access to audit logs are read-only for authorized individuals (privileged accounts only).			

Control Number **AU-10**	**Control Name** **Non-Repudiation**	**Priority** **P2**	**CMS Baseline** **High** **HVA**
Control Statement Provide irrefutable evidence that an individual (or process acting on behalf of an individual)has performed actions to be covered by non-repudiation (defined in applicable system security and privacy plan) and has falsely deny having performed those actions.			
Discussion			

Types of individual actions covered by non-repudiation include creating information, sending and receiving messages, and approving information. Non-repudiation protects against claims by authors of not having authored certain documents, senders of not having transmitted messages, receivers of not having received messages, and signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from an individual or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request, or receiving specific information). Organizations obtain non-repudiation services by employing various techniques or mechanisms, including digital signatures and digital message receipts.	
Implementation Standard	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls
AU-9, PM-12, SA-8,SC-8, SC-12, SC-13, SC-16, SC-17, SC-23
(Redacted Privacy Controls: AR-4 and AR-8)
	Reference Policy
	Code: 5 U.S.C. §552a(e)(5) and (g)(1)(c);
	FISCAM: AC-2, AS-2;
	OMB Circular A-130: 7.g. and 8.b(2)(c)(iii);
	45 C.F.R. §164.308(a)(5)(ii)(C);
	45 C.F.R. §164.312(b);
	45 C.F.R. §164.312(c)(1);
	45 C.F.R. §164.312(c)(2);
	45 C.F.R. §164.312(e)(2)(i);
	FIPS: 140-3, 180-4, 186-4, 202;
	SP 800-177.

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Provide irrefutable evidence that an individual (or process acting on behalf of an individual, users, privileged users, system accounts, and service accounts) has performed a particular action. All accounts, including system and service accounts, are traceable back to an accountable individual.	
HVA Discussion Types of individual actions covered by non-repudiation include creating information, sending and receiving messages, and approving information. Non-repudiation protects against claims by authors of not having authored certain documents, senders of not having transmitted messages, receivers of not having received messages, and signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, or approving a procurement request, or received specific information). Organizations obtain non-repudiation services by employing various techniques or mechanisms, including digital signatures and digital message receipts	
HVA Implementation Standard Implement HVA non-repudiation for users, privileged users, system accounts, and service accounts. Ensure all accounts, include system and service accounts, are traceable back to an accountable individual	

Control Number **AU-11**	**Control Name** **Audit Record Retention**	**Priority** **P3**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement Retain audit records for ninety (90) days and archive old records for one (1) year consistent with records retention policy to provide support for after-the-fact investigations of incidents and to meet regulatory and CMS information retention requirements.			
Discussion			

Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes the retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on records retention.

Implementation Standard

High, Moderate & Low:

Std.1 - When subject to a legal investigation (e.g., Insider Threat), audit records must be maintained until released by the investigating authority.

Std.2 - Audit record retention must comply with National Archives and Records Administration (NARA) or other authoritative mandate durations

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AU-2,AU-4, AU-5, AU-6,AU-9, AU-14,MP-6,RA-5, SI-12.
	Reference Policy
	FedRAMP Rev. 4 Baseline;
	FISCAM: AC-5, AS-2;
	HHS: Policy for Monitoring Employee Use of HHS IT Resources;
	OMB A-130

Privacy Discussion

Privacy Implementation Standards

High & Moderate:

PRIV.1 - Audit inspection reports, including a record of corrective actions, must be retained by the organization for a minimum of three (3) years from the date the inspection was completed.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **AU-12**	**Control Name** **Audit Record Generation**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement

(a). Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on:

- All successful and unsuccessful authorization attempts;
- All changes to logical access control authorities (e.g., rights, permissions);
- All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services;
- The audit trail, which must capture the enabling or disabling of audit report generation services; and
- The audit trail must capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database);

(b). Allow defined personnel or roles (defined in the applicable system security and privacy plan)to select the event types that are to be logged by specific components of the system; and

(c). Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

Discussion

Audit records can be generated from many different system components. The event types specified in AU-2d are the event types for which audit logs are to be generated and are a subset of all event types for which the system can generate audit records.

Implementation Standard

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)
Related Controls	**Reference Policy**

AC-3, AC-6, AC-17,AU-2, AU-3,AU-4, AU-5, AU-6, AU-7,AU-14, CM-5, MA-4, MP-4, PM-12, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10.	FedRAMP Rev. 4 Baseline;
	OMB Circular A-130: 7.g. and 8.b(2)(c)(iii);
	45 C.F.R. §164.308(a)(1)(ii)(D);
	45 C.F.R. §164.308(a)(5)(ii)(C);
	45 C.F.R. §164.312(b)

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AU-12(01)**	**Control Name** **System-Wide and Time-Correlated Audit Trail**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Compile audit records from defined system components (defined in the applicable system security and privacy plan)into a system-wide (logical or physical) audit trail that is time-correlated to within +/- five (5) minutes for the relationship between time stamps of individual records in the audit trail.			
Discussion Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.			
Implementation Standard			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	
Related Controls AU-8, SC-45		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **AU-12(03)**	**Control Name** **Changes by Authorized Individuals**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Provide and implement the capability for defined individuals or roles (defined in the applicable system security and privacy plan)to change the logging to be performed on system components (defined in the applicable system security and privacy plan) based on selectable event criteria (defined in the applicable system security and privacy plan) within minutes.			
Discussion Permitting authorized individuals to make changes to system logging enables organizations to extend or limit logging as necessary to meet organizational requirements. Logging that is limited to conserve system resources may be extended (either temporarily or permanently) to address certain threat situations. In addition, logging may be limited to a specific set of event types to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which logging actions are changed (e.g., near real-time, within minutes, or within hours).			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	

Related Controls
AC-3
	Reference Policy
	OMB Circular A-130: 7.g. and 8.b(2)(c)(iii);
	45 C.F.R. §164.308(a)(1)(ii)(D);
	45 C.F.R. §164.308(a)(5)(ii)(C);
	45 C.F.R. §164.312(b);
	45 C.F.R. §164.308(a)(1)(i);
	45 C.F.R.§164.308(a)(2)

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **AU-16**	**Control Name** **Cross-Organizational Audit Logging**	**Priority** **P3**	**CMS Baseline** **HVA**
Control Statement Employ methods (defined in the applicable system security and privacy plan) for coordinating audit information (defined in the applicable system security and privacy plan) among external organizations when audit information is transmitted across organizational boundaries.			
Discussion When organizations use systems or services of external organizations, the audit logging capability necessitates a coordinated, cross-organization approach. For example, maintaining the identity of individuals who request specific services across organizational boundaries may often be difficult, and doing so may prove to have significant performance and privacy ramifications. Therefore, it is often the case that cross-organizational audit logging simply captures the identity of individuals who issue requests at the initial system, and subsequent systems record that the requests originated from authorized individuals. Organizations consider including processes for coordinating audit information requirements and protection of audit information in information exchange agreements.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	

Related Controls
AU-3, AU-6,AU-7, CA-3, PT-7
		Reference Policy
		45 C.F.R. §164.308(a)(1)(ii)(D);
		45 C.F.R. §164.308(a)(5)(ii)(C);
		45 C.F.R. §164.312(b);
		45 C.F.R. §164.314	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Employ CMS-defined methods (defined in the applicable system security and privacy plan) for coordinating CMS-defined audit information (defined in the applicable system security and privacy plan) among external organizations when audit information is transmitted across organizational boundaries.			
HVA Discussion Organizations using external systems and services to support the HVA maintain auditing capabilities, non-repudiation of the users, and correlation of actions across the external systems to allow for accurate and timely incident response capabilities. Organizations require that the contractor or external hosting entity comply with federal and agency audit requirements in the external environments. The external system provides non-repudiation for non-public user access to HVA information for accountability.			
HVA Implementation Standard Require the contractor or external hosting entity comply with federal and agency audit requirements in the external environments.			

Assessment, Authorization and Monitoring

Control Number	Control Name	Priority	CMS Baseline
CA-01	**Policies and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel or roles:

1. CMS Enterprise-level assessment, authorization, and monitoring policy that:
    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

(c) Review and update the current assessment, authorization, and monitoring:

1. Policy at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines);

Discussion

This control addresses policy and procedures for the controls in the CA family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise level assessment, authorization, and monitoring policy within this ARS, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures.)

Implementation Standard

High, Moderate & Low:

Std.1 - The CIO and CISO will: (a) Develop, document, and disseminate to applicable stakeholder personnel or roles via the IS2P2:

1. CMS Enterprise-level assessment, authorization, and monitoring policy that:
    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

(c) Review and update the current assessment, authorization, and monitoring:

1. Policy at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines);

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years

Related Controls	Reference Policy

PM-9, PS-8, SI-12;
(Redacted Privacy Controls: AR-1 and AR-7)
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-1, SM-3;
	HIPAA: 45 C.F.R. §164.308(a)(8), 45 C.F.R.§164.316(b)(1)(ii), 45 C.F.R. §164.316(b)(2)(ii), 45 C.F.R. §164.308(a)(2);
	HSPD: HSPD 7 F(19);
	NISTIR 8062;
	NIST SP: 800-12, 800-30, 800-37, 800-39, 800-53A, 800-100, 800-137;
	OMB Circular: A-130 Appendix II;
	OMB Memo: M-17-12, Att. 1;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
The assessment, authorization, and monitoring policy and procedures should address the strategy for including applicable privacy requirements and controls in the systems. As such, updates to the assessment, authorization, and monitoring policy and procedures must also address changes in federal privacy laws and policy requirements. Since CMS requires at least every three-year review of the assessment, authorization, and monitoring policy and procedures, the statute driven requirement to review the privacy policy and procedures every two years will be met.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
High & Moderate:
PRIV.1 - Monitor for changes to applicable privacy laws, regulations, and overarching policy that affect assessment, authorization, and monitoring policies no less often than once every 365 days to ensure the CMS and Mission/Business/System affect assessment, authorization, and monitoring policies remains effective.
PRIV.2 - Ensure affect assessment, authorization, and monitoring policies support privacy to the greatest extent feasible throughout the system's life cycle.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
CA-02	**Control Assessments**	**P2**	**Low** **Moderate** **High**

Control Statement

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;
b. Develop a control assessment plan that describes the scope of the assessment including:
1. Controls and control enhancements under assessment within every three hundred sixty-five (365) days in accordance with the CMS Acceptable Risk Safeguards (ARS) and as defined in the implementation standards;
2. Assessment procedures to be used to determine control effectiveness; and
3. Assessment environment, assessment team, and assessment roles and responsibilities;
c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
d. Assess the controls in the system and its environment of operation within every three hundred sixty-five (365) days in accordance with the CMS Acceptable Risk Safeguards (ARS) and as defined in the implementation standards to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
e. Produce a control assessment report that document the results of the assessment; and
f. Provide the results of the control assessment to the Business Owner responsible for the system and personnel responsible for reviewing the assessment documentation, and updating security and privacy documentation where necessary to reflect any changes to the system within thirty (30) days after its completion, in writing.

Discussion

Organizations assess controls in systems and the environments in which those systems operate as part of initial and ongoing authorizations; continuous monitoring; FISMA annual assessments; system design and development; systems security engineering; and the system development life cycle. Assessments help to ensure that organizations meet information security and privacy requirements; identify weaknesses and deficiencies in the system design and development process; provide essential information needed to make risk-based decisions as part of authorization processes; and comply with vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls as documented in security and privacy plans. Assessments can also be conducted throughout the system development life cycle as part of systems engineering and systems security engineering processes. For example, the design for the controls can be assessed as RFPs are developed and responses assessed, and as design reviews are conducted. If design to implement controls and subsequent implementation in accordance with the design is assessed during development, the final control testing can be a simple confirmation utilizing previously completed control assessment and aggregating the outcomes.

Organizations may develop a single, consolidated security and privacy assessment plan for the system or maintain separate plans. A consolidated assessment plan clearly delineates roles and responsibilities for control assessment. If multiple organizations participate in assessing a system, a coordinated approach can reduce redundancies and associated costs.

Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security and privacy posture of systems during the system life cycle. Assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, senior agency information security officers, and authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations; continuous monitoring; systems engineering processes, or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits, including audits by external entities such as regulatory agencies, are outside the scope of this control.

Implementation Standard

High, Moderate & Low:

Std.1 - An assessment of all controls must be conducted [by an independent third-party security control assessor] prior to issuing the initial authority to operate for all newly implemented systems or systems requiring re-authorization.

Std.2 - The annual assessment requirement mandated by OMB requires all baseline controls, defined in the CMS Minimum Security Requirements (CMSRs), attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the CMSRs must be tested each year so that all controls are tested during a 3-year period.

Std.3 - The Business Owner notifies the CMS CISO within thirty (30) days whenever updates are made to system authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, Information System Security Officer [ISSO]).

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-20, CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SC-38, SI-3, SI-4, SI-12, SR-2, SR-3;
(Redacted Privacy Controls: AR-2)
	Reference Policy
	Code: 5 U.S.C. §552a(b);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	Executive Order: 13587;
	FedRAMP: Rev. 4 Baseline;
	FIPS: 199;
	FISCAM: AS-1, SM-5;
	HIPAA: 45 C.F.R. §164.308(a)(8);
	HSPD: HSPD 7 D(11) F(19);

	NISTIR: 8062;
	NIST SP: 800-18, 800-37, 800-39, 800-53A, 800-115, 800-137;
	OMB Circular: A-130;
	OMB Memo: M-17-12 Att. 1, A.2.c, M-14-03, M-15-01, M-16-04, M-19-03;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

This control addresses the process of planning for and executing control assessments, the scope of which should include assessment of applicable privacy requirements. Privacy Impact Assessments (PIAs) are structured reviews (qualitative and quantitative) of both the risk and effect of how information is handled and maintained as well as the potential impacts or harms to individuals and organizations (to include CMS and CMS Businesses/Systems) for loss of control or mishandling of the PII. The term "PIA" may refer to the process of conducting such an assessment, or the document produced as a result of that assessment. Once the final control assessment is completed, update the associated Privacy Impact Assessment (PIA) to reflect the results of the assessment.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Conduct Privacy Impact Assessment (PIA) to assess privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII or other activities that pose a privacy risk to CMS systems in accordance with applicable law, OMB policy, or any existing CMS or CMS Business/System policies and procedures; and;

PRIV.2 - Review and update the associated Privacy Impact Assessment (PIA) to reflect the results of the control assessment no less than every three (3) years..

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CA-02(01)	**Independent Assessors**	**P2**	**Moderate** **High**

Control Statement

Employ independent assessors or assessment teams with CMS CISO defined level of independence to conduct control assessments.

Discussion

Independent assessors or assessment teams are individuals or groups conducting impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted; assess their own work; act as management or employees of the organizations they are serving; or place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. Assessor independence determination also includes whether contracted assessment services have sufficient independence, for example, when system owners are not directly involved in contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, the analogy to independent assessors is having independent SMEs involved in design reviews.

When organizations that own the systems are small or the structures of the organizations require that assessments are conducted by individuals that are in the developmental, operational, or management chain of the system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Assessments performed for purposes other than to support authorization decisions, are more likely to be useable for such decisions when performed by assessors with sufficient independence, thereby reducing the need to repeat assessments.

Implementation Standard

High, Moderate & Low: Std.1 - The CISO will employ independent third-party security control assessors or assessment teams with a CMS CISO defined level of independence to conduct control assessments.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls None;	**Reference Policy** FedRAMP: Rev. 4 Baseline
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **CA-02(02)**	**Control Name** **Specialized Assessments**	**Priority** **P2**	**CMS Baseline** **High**

Control Statement Include as part of control assessments, within every three hundred sixty-five (365) days, announced or unannounced in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment.	
Discussion Organizations can conduct specialized assessments, including verification and validation, system monitoring, insider threat assessments, malicious user testing, and other forms of testing. These assessments can improve readiness by exercising organizational capabilities and indicating current levels of performance as a means of focusing actions to improve security and privacy. Organizations conduct specialized assessments in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can include vulnerabilities uncovered during assessments into vulnerability remediation processes. Specialized assessments can also be conducted early in the system development life cycle, for example, during design, development, and unit testing. Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.	
Implementation Standard High & Moderate: Std.1 - The CCIC will perform: 1 - Announced or unannounced in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, [and performance/load testing results] that must be searchable by the CCIC: (a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; (b) In-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, [and performance/load testing result] information sources include traffic analysis tool systems, appliances, devices, services, and applications; and (c) CCIC directed in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, [and performance/load testing] information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.2 - As required by CMS, raw results from in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, [and performance/load testing] must be available in an unaltered format to the CCIC. Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
PE-3, SI-2;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	NIST SP: 800-37, 800-39, 800-115, 800-137;

	OMB Memo: M-14-03, M-15-01, M-16-04, M-19-03;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number CA-02(03)	**Control Name** **LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS**	**Priority** **P2**	**CMS Baseline** **High**
Control Statement Leverage the results of control assessments performed by CMS authorized independent assessors on CMS systems when the assessment meets CMS defined requirements and methodologies for performing assessments.			
Discussion Organizations may rely on control assessments of organizational systems by other (external) organizations. Using such assessments and reusing existing assessment evidence can decrease the time and resources required for assessments by limiting the independent assessment activities that organizations need to perform. The factors that organizations consider in determining whether to accept assessment results from external organizations can vary. Such factors include the organization's past experience with the organization that conducted the assessment; the reputation of the assessment organization; the level of detail of supporting assessment evidence provided; and mandates imposed by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Accredited testing laboratories supporting the Common Criteria Program [ISO 15408-1], the NIST Cryptographic Module Validation Program (CMVP), or the NIST Cryptographic Algorithm Validation Program (CAVP) can provide independent assessment results that organizations can leverage.			
Implementation Standard High, Moderate & Low: Std.1 - The CISO will leverage the results of control assessments performed by CMS authorized independent third-party security control assessors on CMS systems when the assessment meets CMS defined requirements and methodologies for performing assessments. 1 - The results from the control assessments producing any documented vulnerabilities or weakness for the identified system(s) via the Security Assessment Report (SAR) must feed into the CMS Plan of Action and Milestones (POA&M) program for tracking and remediation in CFACTS.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
SA-4;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		NIST SP: 800-37, 800-39, 800-137;
		OMB Memo: M-14-03, M-15-01, M-16-04, M-19-03;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CA-03**	**Control Name** **Information Exchange**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**

Control Statement

(a) Approve and manage the exchange of information between the system and other systems using: interconnection security agreements (ISA); information exchange security agreements; memoranda of understanding or agreement (MOU/MOA); service level agreements (SLA); and other exchange agreements (defined in applicable security and privacy plans)
(b) Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
(c) Review and update the agreements no less often than once every year (365 days) and whenever significant changes (that can affect the security and privacy state of the system) are implemented that could impact the validity of the agreement as a verification of enforcement of security and privacy requirements.

Discussion

System information exchange requirements apply to information exchanges between two or more systems. System information exchanges include connections via leased lines or virtual private networks, connections to internet service providers, database sharing or exchanges of database transaction information, connections and exchanges associated with cloud services, exchanges via web-based services, or exchanges of files via file transfer protocols, network protocols (e.g., IPv4, IPv6), email, or other organization to organization communications. Organizations consider the risk related to new or increased threats, that may be introduced when systems exchange information with other systems that may have different security and privacy requirements and controls. This includes systems within the same organization and systems that are external to the organization. A joint authorization of the systems exchanging information as described in CA-6(1) or CA-6(2) may help to communicate and reduce risk.
Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The type of agreement selected is based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system. If systems that exchange information have the same authorizing official, organizations need not develop agreements. Instead, the interface characteristics between the systems (e.g., how the information is being exchanged; how the information is protected) are described in the respective security and privacy plans. If the systems that exchange information have different authorizing officials within the same organization, the organizations can develop agreements, or they can provide the same information that would be provided in the appropriate agreement type from CA-3a in the respective security and privacy plans for the systems. Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (including service providers, contractors, system developers, and system integrators). Risk considerations include systems sharing the same networks.

Implementation Standard

High, Moderate & Low:

Std.1 - If the interconnecting systems have the same AO (or same primary operational IT infrastructure manager), an interconnection security agreement document is not required; rather, the interface characteristics between the interconnecting information systems are described in the security and privacy plans (SSP) for the respective systems.
Std.2 - Record each system interconnection in the applicable security plan and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.
Std.3 - The interconnection agreement (or other applicable connection agreement) is updated following significant or major changes to the system, organizations, or the nature of the electronic sharing of information that could impact the validity or security postures of the agreement.
Std.4 - The CMS CIO, CISO, and Senior Official for Privacy (SOP) have the authority to order the immediate termination and/or suspension of any interconnection that, in the judgment of the CMS official and CMS Security Operations, presents an unacceptable level of risk to the CMS enterprise and/or mission.
Std.5 - The interconnection agreement must be fully signed and executed prior to any interconnection outside of the system or authorization boundary taking place for any purpose (within the constraints of the control [e.g., dedicated connections], including testing). Std. 6 - The ISA and any supporting documentation must be uploaded into CFACTS for incorporation into the security artifacts library prior to authorization and review by the AO.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-6, CA-7, IA-3, IR-4, PL-2, PT-8, RA-3, SA-9, SC-7, SI-4, SI-12;
	Reference Policy
	Code: 5 U.S.C. §552a(o);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FIPS: 199;

	FISCAM: AC-1, AS-2;
	HIPAA: 45 C.F.R. §164.308(b)(1), 45 C.F.R. §164.308(b)(4), 45 C.F.R. §164.314(a)(2)(ii), 45 C.F.R. §164.308(b)(3), 45 C.F.R. §164.504(e)(3);
	HSPD: NSPD 7 F(19);
	NIST SP: 800-47;
	OMB Circular: A-130 Appendix II;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

System information exchange requirements apply to information exchanges between two or more systems. Interconnection agreements document whether and under what circumstances sensitive information, such as personally identifiable information (PII), can be shared between systems in different authorization boundaries (e.g., an interface between systems owned by different agencies) over a dedicated or “always on” connection. Interconnection agreements communicate that sensitive information will be communicated via the connection and define the security parameters required to protect it. Interconnection agreements also provide a record of agreed upon terms and a document against which controls can be enforced and audited. CMS and CMS Business/System policy dictates whether interconnection agreements are required for internal connections within CMS or the System.

Discussion for systems processing, storing, or transmitting PHI:

Consider the need for a MOU/MOA or Business Associate Agreement, and implement as necessary. Under HIPAA Privacy Rule, a covered entity may not use, disclose or request a medical record, except when the medical record is specifically justified and reasonably necessary to accomplish the purpose of the use, disclosure, or request. The disclosure and sharing of PHI is governed by the HIPAA regulations.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Enters into MOUs, MOAs, Letters of Intent, CMAs, or similar agreements, with parties (internal and external) that specifically describe the PII covered and enumerate the purposes for which the PII may be used.

PRIV.2 - Consistent with the Purpose Specification and Use Limitation Fair Information Practice Principles (FIPPs), sharing of PII must be compatible with the purpose for which it was collected. Consistent with the Transparency FIPP, any subsequent sharing that is not compatible may not be done until additional notice is provided to the individual, their consent is obtained, and relevant documents are updated or published; e.g., when applicable and

Systems processing, storing, or transmitting PHI:

High & Moderate:

PHI.1 - Consider the need for a MOU/MOA or Business Associate Agreement, and implement as necessary.

HVA Control Statement

(a) Approve and manage the exchange of information between the system and other systems using: interconnection security agreements (ISA); information exchange security agreements; memoranda of understanding or agreement (MOU/MOA); service level agreements (SLA); and other exchange agreements (defined in applicable security and privacy plans)

(b) Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

(c) Review and update ISAs and MOUs at least annually and in response to environmental or operational changes to either system.

HVA Discussion

Organizations should create, authorize, and track ISA documents for each external support services and each external connection (outside the authorization boundary) to and from the HVA. In the case of external connections, the ISA includes technical details to include but not limited to: IP addresses, Doman Name System (DNS) names, protocols, ports, frequency of transfers, incident response contacts at both organizations, description of data exchanged, direction of data exchange, sensitive level of data exchanged, security categorization of both systems, and ATO status.

For external support services the ISA minimally includes service description, expected availability (uptime) of the service, technical point of contacts, incident response contacts at both organizations, importance of the external service, security categorization of both systems, and ATO status.

HVA Implementation Standard

Systems designated as HVA:
High & Moderate:
HVA.1 – Approve and manage the exchange of HVA information with external entities using interconnection security agreements (ISAs) and memoranda of understanding or agreement (MOU/As).
HVA.2 – Review and update ISA and MOU/A at least annually and in response to environmental or operational changes to either system.

Control Number	Control Name	Priority	CMS Baseline
CA-05	**Plan of Action and Milestones**	**P3**	**Low** **Moderate** **High** **HVA**

Control Statement

(a) Develop a plan of action and milestones (POA&M) for the system (for every internal/external audit/review or test (e.g., Security Control Assessment [SCA], penetration test, automated configuration and vulnerability scan results) to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
(b) Update existing plan of action and milestones (POA&M) every 3 months (Quarterly) until all the findings are resolved based on the findings from control assessments, audits, and continuous monitoring activities.

Discussion

Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are required in authorization packages and are subject to federal reporting requirements established by OMB.

Implementation Standard

High, Moderate & Low:

Std.1 - The Business Owner and ISSO of the FISMA system will: (a) Develop a plan of action and milestones (POA&M) based on the HHS Standard for Plan of Action and Milestones (POAM) Management and Reporting, and the CMS Plan of Action and Milestones Process Guide for the FISMA system (for every internal/external audit/review or test (e.g., Security Control Assessment [SCA], penetration test, automated configuration and vulnerability scan results) to document the planned remediation actions of the FISMA system to correct any weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
(b) Update existing plan of action and milestones (POA&M) every 3 months (Quarterly) until all the findings are resolved or remediated based on the findings from control assessments, audits, and continuous monitoring activities.

Control Review Frequency	Assessment Frequency
Quarterly	Annually (365 Days)
Related Controls	**Reference Policy**

CA-2, CA-7, CM-4, PM-4, PM-9, RA-7, SI-2, SI-12;	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-6;
	HIPAA: 45 C.F.R. §164.308(a)(2), 45 C.F.R. §164.308(a)(8);
	HSPD: HSPD 7 F(19), G(24);
	NIST SP: 800-37, 800-39, 800-115, 800-137;
	OMB Circular: A-130;
	OMB Memo: M-02-01, M-14-03, M-15-01, M-16-04, M-19-03;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a) Develop a plan of action and milestones (POA&M) for the system (for every internal/external audit/review or test (e.g., Security Control Assessment [SCA], penetration test, automated configuration and vulnerability scan results) to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
(b) Review and update the HVA systems and supporting system's POA&M at least monthly, and ensure it is signed off by the AOs [dual AOs - see AU-9(5)] at least quarterly.

HVA Discussion

HVA systems are to be prioritized for timely remediation of weaknesses and deficiencies to minimize the risks to the HVA. Organizations should prioritize remediation efforts based on the risk to the systems to remediate highest risks first. Prioritized POA&M management informs the planning, programming, budgeting and execution (PPBE) cycles associated with remediation and/or aligned with development modernization enhancement (DME) projects. agencies ensure that adequate and timely resources are allocated to support remediation efforts. All supporting system weaknesses and deficiencies are tracked and reviewed by HVA Authorizing Officials to ensure systems risks are remediated expeditiously.

HVA Implementation Standard

Systems designated as HVA:
High & Moderate:
HVA.1 – Review and update HVA systems and supporting system’s Plan of Action and Milestones (POA&M) at least monthly [thirty (30) days]
HVA.2 – Enforce dual authorization, two appropriate organizational personnel such as CMS-defined officials (e.g., CMS Senior Management such as the AO, CISO, SOP) and organization defined officials (e.g., Business Owner, System Owner, ISSO) for signing off on HVA systems and supporting system’s Plan of Action and Milestones (POA&M) at least quarterly.

Control Number	Control Name	Priority	CMS Baseline
CA-06	**Authorization**	**P3**	**Low** **Moderate** **High** **HVA**

Control Statement

(a) Assign a senior official as the authorizing official for the system;
(b) Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;
(c) Ensure that the authorizing official for the system, before commencing operations:
1. Accepts the use of common controls inherited by the system; and
2. Authorizes the system to operate;
(d) Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
(e) Update the authorizations within every three (3) years and:
- When significant changes are made to the system;
- When changes in requirements result in the need to process data of a higher sensitivity;
- When changes occur to authorizing legislation or federal requirements that impact the system;
- After the occurrence of a serious security and privacy violation which raises questions about the validity of an earlier authorization; and
- Prior to expiration of a previous authorization.

Discussion

Authorizations are official management decisions by senior officials [CMS CIO or his/her designated representative (i.e., authorizing officials)] to authorize operation of systems, to authorize the use of common controls for inheritance by organizational systems and to explicitly accept the risk to CMS operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon controls. Authorizing officials provide budgetary oversight for organizational systems and for common controls or assume responsibility for the mission and business operations supported by those systems or common controls. The authorization process is a federal responsibility and therefore, authorizing officials must be federal employees. Authorizing officials are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems. Nonfederal organizations may have similar processes to authorize systems and senior officials that assume the authorization role and associated responsibilities.

Authorizing officials issue ongoing authorizations of systems based on evidence produced from implemented continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes. Through the employment of comprehensive continuous monitoring processes, the information contained in authorization packages (i.e., the security and privacy plans, assessment reports, and plans of action and milestones), is updated on an ongoing basis. This provides authorizing officials, system owners, and common control providers with an up-to-date status of the security and privacy posture of their systems, controls, and operating environments. To reduce the cost of reauthorization, authorizing officials can leverage the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

Implementation Standard

High, Moderate & Low:

Std.1 - (a) Assign a senior official as the authorizing official (AO) for the system;

(b) Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

(c) Ensure that the authorizing official for the system(s), before commencing operations:

1. Accepts the use of common controls inherited by the system; and
2. Authorizes the system to operate;

(d) Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;

(e) Update the authorizations at a minimum within every three (3) years and:

- When significant or major changes are made to the system;
- When changes in requirements result in the need to process data of a higher sensitivity;
- When changes occur to authorizing legislation or federal requirements that impact the system;
- After the occurrence of a serious security and privacy violation which raises questions about the validity of an earlier authorization; and
- Prior to expiration of a previous authorization.

Std. 2 The Business Owner and/or ISSO of the FISMA system must notify the CCIC of significant or major changes to architecture, security and privacy posture, or other items that could cause degradation or unexpected results in security and privacy monitoring, detection, response, and mitigation activities prior to making a change.

Control Review Frequency	**Assessment Frequency**
Three (3) Years	Three (3) Years

Related Controls	**Reference Policy**

CA-1, CA-2, CA-3, CA-7, PM-9, PM-10, SA-10, SI-12;	Code: 5 U.S.C. §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	Pub. L. No. 107-347, §208;
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS- 1, SM-2;
	HIPAA: 45 C.F.R. §164.308(a)(2), 45 C.F.R. §164.308(a)(8), 45 C.F.R. §164.316(b)(2)(iii);
	HSPD: HSPD 7 F(19);
	NIST SP: 800-37, 800-39, 800-137;
	OMB Circular: A-130;
	OMB Memo: M-11-33, M-14-03, M-15-01, M-16-04, M-19-03;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

One of the considerations for the “go/no go” decision when authorizing (or re-authorizing) an system is whether applicable privacy requirements have been met.

Discussion for systems processing, storing, or transmitting PHI:

The senior-level executive should be one of the following: HIPAA Security Officer, Authorizing Official, Program Manager, Information System Security Manager (ISSM), or Information System Security Officer (ISSO).

Privacy Implementation Standards

HVA Control Statement

(a) Assign a senior official as the authorizing official for the HVA;

(b) Assign a senior official as the authorizing official for common controls available for inheritance by organizational HVAs;
(c) Ensure that the authorizing official for the HVA, before commencing operations:
1.Accepts the use of common controls inherited by the HVA and
2. Authorizes the HVA to operate;
(d) Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
(e) Update the authorizations within every three (3) years and:

- When significant changes are made to the system;
- When changes in requirements result in the need to process data of a higher sensitivity;
- When changes occur to authorizing legislation or federal requirements that impact the system;
- After the occurrence of a serious security and privacy violation which raises questions about the validity of an earlier authorization; and
- Prior to expiration of a previous authorization.

HVA Discussion

The AO must completely understand the risks, to the organization and Nation, of operating the HVA. The Security Control Assessment process is inclusive of all identified risks from systems, components, information, interconnections, users, vulnerabilities, and threats. If the Security Control Assessment results in a pre-determined unacceptable level of residual risk to the system, the organization should remediate issues to reduce the risk to an acceptable level or rescinds the HVAs ATO. Omitting information from the Security Control Assessment could result in this decision process being conducted with inaccurate or incomplete information leading to the HVA operating in an unknown risk state.

HVA Implementation Standard

Systems designated as HVA:
High & Moderate:
HVA.1 – Ensure AO understand the risks posed by HVAs and the related organizational responsibilities as part of the authorization process.

Control Number	Control Name	Priority	CMS Baseline
CA-06(01)	**Joint Authorization Intra-Organization**		**HVA**

Control Statement

Employ a joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization.

Discussion

Assigning multiple authorizing officials from the same organization to serve as co-authorizing officials for the system, increases the level of independence in the risk-based decision-making process. It also implements the concepts of separation of duties and dual authorization as applied to the system authorization process. The intra-organization joint authorization process is most relevant for connected systems, shared systems, and systems with multiple information owners

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**
AC-6;	See CA-6;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

Employ a joint authorization process for the HVA that includes multiple AOs from the same organization conducting the authorization.

HVA Discussion

The HVA authorization process represents all HVA dependent functions/missions in the authorization process to ensure that risk-based decisions are transparent and reflective of the risk-tolerance of all missions that are reliant on the HVA. The joint authorization process makes it clear that co-AOs are equally responsible for authorizing and accepting risks to the HVA system. All system documentation that is typically required to be signed by the AO is to be signed by both co-AOs for this system.

HVA Implementation Standard

Systems designated as HVA:
High & Moderate:
HVA.1 - Assign joint AOs from the same organization to serve as co-AOs for the HVA system.

HVA.2 - Ensure all system documentation that is typically required to be signed by the AO is to be signed by both co-AOs for the HVA system.

Control Number	Control Name	Priority	CMS Baseline
CA-07	**Continuous Monitoring**	**P3**	**Low** **Moderate** **High** **HVA**

Control Statement

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

(a) Establishing system-level metrics to be monitored (defined in the applicable system security and privacy plan) based on the organization security and privacy goals and in accordance with NIST SP 800-137 "Information Security Continuous Monitoring (ISCM)";

(b) Establishing defined frequencies (defined in the applicable system security and privacy plan), but no less than once every 72 hours for monitoring and defined frequencies (defined in the applicable system security and privacy plan), but no less than once every 72 hours for assessment of control effectiveness;

(c) Ongoing control assessments in accordance with the continuous monitoring strategy;

(d) Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

(e) Correlation and analysis of information generated by control assessments and monitoring;

(f) Response actions to address results of the analysis of control assessment and monitoring information; and

(g) Reporting the security and privacy status of the system to defined personnel or roles (defined in the applicable system security and privacy plan) every thirty (30) days [monthly].

Discussion

Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives organizational officials the ability to make effective and timely risk management decisions, including ongoing authorization decisions.

Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems. Monitoring requirements, including the need for specific monitoring, may be referenced in other controls and control enhancements, for example, AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PM-31, PS-7e, SA-9c, SR-4, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18c, SC-43b, SI-4.

Implementation Standard

High, Moderate & Low:

Std. 1 - The CIO and CISO will develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

(a) Establishing system-level metrics to be monitored (defined in the applicable system security and privacy plan) based on the organization security and privacy goals and in accordance with NIST SP 800-137 "Information Security Continuous Monitoring (ISCM)";

(b) Establishing defined frequencies (defined in the applicable system security and privacy plan), but no less than once every 72 hours for monitoring and defined frequencies (defined in the applicable system security and privacy plan), but no less than once every 72 hours for assessment of control effectiveness;

(c) Ongoing control assessments in accordance with the continuous monitoring strategy;

(d) Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
(e) Correlation and analysis of information generated by control assessments and monitoring;
(f) Response actions to address results of the analysis of control assessment and monitoring information; and
(g) Reporting the security and privacy status of the system to defined personnel or roles (defined in the applicable system security and privacy plan) every thirty (30) days [monthly]. (h). The CCIC will be the responsible agent to perform the above activities on behalf of the CIO and CISO. Std.2 - The CCIC will ensure the following: 1 - When subject to a legal investigation (e.g., of an insider threat), continuous monitoring records must be maintained until released by the investigating authority.
2 - Monitors systems, appliances, devices, and applications (including databases).
3 - Provides oversight of information security and privacy, to include Security Information and Event Management (SIEM), for each FISMA System operating by or on behalf of CMS.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-7, PT-8, RA-3, RA-5, RA-7, SA-8, SA-9, SA-
	Reference Policy
	Code: 5 U.S.C. §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-5;
	HHS: Policy for Monitoring Employee Use of HHS IT Resources;
	HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(8), 45 C.F.R. §164.308(a)(5)(ii)(C);
	HSPD: HSPD 7 F(19);
	NISTIR: 8011v1, 8062;
	NIST SP: 800-37, 800-39, 800-53A, 800-115, 800-137;
	OMB Circular: A-130;
	OMB Memo: M-11-33, M-14-03, M-15-01, M-16-04, M-19-03;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
The state of controls can directly correlate to privacy risk. Continuous monitoring supports the identification of issues that could result in unauthorized access to sensitive information such as PII, data quality issues, and other concerns, including privacy, that are supported by security controls.
Discussion for systems processing, storing, or transmitting PHI:
Consider using automated tools and mechanisms for system activity review. The effectiveness of continuous monitoring of various activities, for example, failed or successful log-ins, inappropriate file access, detecting and reporting on malicious code/viruses through network transmission, is enhanced using approved automated tools.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
High & Moderate:
PRIV.1 - Monitor privacy controls on systems processing, storing, or transmitting PII to ensure effective implementation in accordance with the continuous monitoring strategy
PRIV.2 - Document, track, and ensure mitigation of corrective actions identified through continuous monitoring.

HVA Control Statement

Develop a HVA system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level information security continuous monitoring strategy that includes:
(a) Establishing system-level metrics to be monitored (defined in the applicable system security and privacy plan) based on the organization security and privacy goals and in accordance with NIST SP 800-137 "Information Security Continuous Monitoring (ISCM)";
(b) Establishing defined frequencies (defined in the applicable system security and privacy plan), but no less than once every 72 hours for monitoring and defined frequencies (defined in the applicable system security and privacy plan), but no less than once every 72 hours for assessment of control effectiveness;
(c) Ongoing control assessments in accordance with the continuous monitoring strategy;
(d) Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

(e) Correlation and analysis of information generated by control assessments and monitoring;
(f) Response actions to address results of the analysis of control assessment and monitoring information; and
(g) Reporting the security and privacy status of the system to defined personnel or roles (defined in the applicable system security and privacy plan) every thirty (30) days [monthly].

HVA Discussion

Continuous Monitoring provides continuous assurance that security controls are effectively meeting organizational protection needs. Organizations should develop a continuous monitoring strategy in accordance with NIST SP 800-137 "ISCM" to include all selected security controls in use for the systems.

The ISCM strategy is maintained to address information security risks and requirements across the organizational risk management tiers. The ISCM strategy is implemented and updated, in accordance with an organization-defined frequency, to reflect the effectiveness of deployed controls, significant changes to information systems, and adherence to federal statutes, policies, directives, instructions, regulations, standards, and guidelines. Use of automated tools and mechanisms is prioritized where possible.

Continuous Monitoring programs follow federal guidance and reporting requirements per OMB Circular A-130 "Managing Information as a Strategic Resource" and comply with Continuous Diagnostics and Mitigation (CDM) reporting requirements. External service providers hosting HVA information and mission critical services are required to meet federal, CISA CDM, and organizational ISCM requirements. The organization should leverage ISCM capabilities to support the migration to the ongoing authorization (OA) process.

HVA Implementation Standard

Systems designated as HVA:
High & Moderate:
HVA.1 - Conduct continuous monitoring activities of HVA systems on an ongoing basis to promote timely risk awareness and remediation
HVA.2 - Employ automated tools and mechanisms to conduct ongoing technical control assessments of HVA systems

Control Number	Control Name	Priority	CMS Baseline
CA-07(01)	**Independent Assessment**	**P2**	**Moderate** **High**

Control Statement

Employ independent assessors or assessment teams with CMS CISO defined level of independence to monitor the controls in the system on an ongoing basis.

Discussion

Organizations maximize the value of control assessments by requiring that assessments be conducted by assessors with appropriate levels of independence. The level of required independence is based on organizational continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted; assess their own work; act as management or employees of the organizations they are serving; or place themselves in advocacy positions for the organizations acquiring their services.

An independent assessor (defined in the RMH, Volume 1, Chapter 10, CMS Risk Management Terms, Definitions, and Acronyms) may be any internal/external agent or team that can conduct an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management chain-of-command associated with the information system or to the determination of control effectiveness. Since these determinations are somewhat subjective, the CMS CISO retains the ultimate authority to make final judgments on the independence of any assessor.

Implementation Standard

High, Moderate & Low:
Std. 1 - The CCIC will act as the independent assessor or assessment team that meets the CMS CISO defined level of independence to monitor the controls in the system on an ongoing basis.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)
Related Controls	**Reference Policy**

AC-9, CA-2;	FedRAMP: Rev. 4 Baseline;
	HSPD: HSPD 7 F(19);
	NIST SP: 800-37, 800-39, 800-137;

	OMB Memo: M-14-03, M-15-01, M-16-04, M-19-03;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **CA-07(03)**	**Control Name** **Trend Analyses**	**Priority** **P3**	**CMS Baseline** **HVA**
Control Statement Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.			
Discussion Trend analyses include examining recent threat information addressing the types of threat events that have occurred within the organization or the federal government; success rates of certain types of attacks; emerging vulnerabilities in technologies; evolving social engineering techniques; the effectiveness of configuration settings; results from multiple control assessments; and findings from Inspectors General or auditors.			
Implementation Standard High, Moderate & Low: Std. 1 - The CCIC will deploy trend analyses techniques to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	

Related Controls
None;
		Reference Policy
		OMB Memo: M-11-33;
		NIST SP: 800-37, 800-39, 800-53A, 800-115, 800-137;
		US-CERT Technical Cyber Security Alerts;
		DoD Information Assurance Vulnerability Alerts;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.			
HVA Discussion Trend analyses include examining recent threat information addressing the types of threat events that have occurred within the organization or the Federal Government; success rates of certain types of attacks; emerging vulnerabilities in technologies; evolving social engineering techniques; the effectiveness of configuration settings; results from multiple control assessments; and findings from Inspectors General or auditors.			
HVA Implementation Standard Systems designated as HVA: High & Moderate: HVA.1 - Examine, correlate, and analyze current threat information sources, emerging vulnerabilities and exploits, latest social engineering tactics, intrusion detection events, and auditor reports on HVA systems.			

Control Number	Control Name	Priority	CMS Baseline
CA-07(04)	**Risk Monitoring**		**Low** **Moderate** **High**

Control Statement

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

(a) Effectiveness monitoring;

(b) Compliance monitoring; and

(c) Change monitoring.

Discussion

Risk monitoring is informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

Implementation Standard

High, Moderate & Low:

Std. 1 - The CCIC will perform risk monitoring as an integral part of the continuous monitoring strategy that includes the following:

(a) Effectiveness monitoring;

(b) Compliance monitoring; and

(c) Change monitoring.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**
None;	See CA-7;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
CA-08	**Penetration Testing**	**P2**	**Moderate** **High**

Control Statement

Conduct penetration testing within every three hundred sixty-five (365) days on defined systems or system components (defined in the applicable system security and privacy plan), or whenever there is a significant change to the system or system components.

Discussion

Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries in carrying out attacks and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies. Penetration testing is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes pretest analysis based on full knowledge of the system; pretest identification of potential vulnerabilities based on pretest analysis; and testing designed to determine exploitability of vulnerabilities. All

parties agree to the rules of engagement before commencement of penetration testing scenarios. Organizations correlate the rules of engagement for the penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries. Risk assessments guide the decisions on the level of independence required for the personnel conducting penetration testing.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Implementation Standard

High:
Std.1 -Conduct internal and external penetration testing as needed but no less often than once every three hundred sixty-five (365) days in accordance with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements.
Std.2 - Penetration tests are performed when new risks and threats potentially affecting the system/applications are identified and reported or upon request from CMS.
Std.3 - Penetration test scanning includes evaluation of embedded structures (e.g., content that can be changed without reloading the anchor content) and interactive content.
Std.4 - Penetration test scanning results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Penetration test information sources include systems, appliances, devices, services, and applications (including databases).
(c) CCIC directed penetration test information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.5 - Penetration testing on a production system must be conducted in a manner that minimized risk of information corruption or service outage.
Std.6 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.
Moderate & Low:
Std.1 – Conduct internal and external penetration testing as needed but no less often than once every three hundred sixty-five (365) days in accordance with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements.
Std.2 – When selected, penetration tests are performed when new risks and threats potentially affecting the system/applications are identified and reported or upon request from CMS.
Std.3 – When selected, penetration test scanning includes evaluation of embedded structures (e.g., content that can be changed without reloading the anchor content) and interactive content.
Std.4 – When selected, penetration test scanning results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Penetration test information sources include systems, appliances, devices, services, and applications (including databases).
(c) CCIC directed penetration test information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.5 – When selected, penetration testing on a production system must be conducted in a manner that minimizes the risk of information corruption or service outage.
Std.6 – When selected, raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Control Review Frequency Two (2) years	**Assessment Frequency** Annually (365 Days)

Related Controls
SA-11, SA-12, SR-5, SR-6;
(Redacted Privacy Controls: AP-1, AP-2, TR-1, TR-2)
	Reference Policy
	Code: 5 U.S.C. §552a(b) and (e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	NIST SP: 800-115;
	OMB Circular: A-130 7.g. and 8.b(3);
	OMB Memo: M-14-03, M-15-01, M-16-04, M-19-03;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
When user session information and other PII is captured or recorded during penetration testing, ensure relevant privacy controls are addressed.

<table>
<tr><td>Privacy Implementation Standards
Systems processing, storing, or transmitting PII (to include PHI):
High & Moderate:
PRIV.1 - Document the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of penetration testing.
PRIV.2 - Ensure and document the authorized purpose(s) for which PII is collected, used, maintained, and shared in support of penetration testing.</td></tr>
<tr><td>HVA Control Statement</td></tr>
<tr><td>HVA Discussion</td></tr>
<tr><td>HVA Implementation Standard</td></tr>
</table>

<table>
<tr><td>Control Number
CA-08(01)</td><td colspan="2">Control Name
Independent Penetration Testing Agent or Team</td><td>Priority
P3</td><td>CMS Baseline
Above Baseline</td></tr>
<tr><td colspan="5">Control Statement
Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.</td></tr>
<tr><td colspan="5">Discussion
Independent penetration testing agents or teams are individuals or groups who conduct impartial penetration testing of organizational systems. Impartiality implies that penetration testing agents or teams are free from perceived or actual conflicts of interest with respect to the development, operation, or management of the systems that are the targets of the penetration testing. CA-2(1) provides additional information on independent assessments that can be applied to penetration testing.</td></tr>
<tr><td colspan="5">Implementation Standard
High & Moderate:
Std.1 - The independent penetration agent or penetration team must be a CMS CISO approved independent penetration test vendor.</td></tr>
<tr><td colspan="2">Control Review Frequency
Not Specified</td><td colspan="3">Assessment Frequency
Three (3) Years</td></tr>
<tr><td colspan="2">Related Controls
CA-2;</td><td colspan="3">Reference Policy
FedRAMP: Rev. 4 Baseline;
NIST SP: 800-115;
OMB Memo: M-14-03, M-15-01, M-16-04, M-19-03;</td></tr>
<tr><td colspan="5">Privacy Discussion</td></tr>
<tr><td colspan="5">Privacy Implementation Standards</td></tr>
<tr><td colspan="5">HVA Control Statement</td></tr>
<tr><td colspan="5">HVA Discussion</td></tr>
<tr><td colspan="5">HVA Implementation Standard</td></tr>
</table>

<table>
<tr><td>Control Number
CA-08(02)</td><td colspan="2">Control Name
RED TEAM EXERCISES</td><td>Priority</td><td>CMS Baseline
Above Baseline</td></tr>
<tr><td colspan="5">Control Statement
Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [MAC-defined red team exercises].</td></tr>
<tr><td colspan="5">Discussion</td></tr>
<tr><td colspan="5">Implementation Standard</td></tr>
<tr><td colspan="2">Control Review Frequency
Not Specified</td><td colspan="3">Assessment Frequency
Three (3) Years</td></tr>
<tr><td colspan="2">Related Controls
None;</td><td colspan="3">Reference Policy</td></tr>
<tr><td colspan="5">Privacy Discussion</td></tr>
<tr><td colspan="5">Privacy Implementation Standards</td></tr>
<tr><td colspan="5">HVA Control Statement</td></tr>
<tr><td colspan="5">HVA Discussion</td></tr>
</table>

HVA Implementation Standard

Control Number **CA-08(03)**	**Control Name** **Facility Penetration Testing**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Employ a penetration testing process, announced and unannounced, that includes attempts to bypass or circumvent controls associated with physical access points to the facility within every three hundred sixty-five (365) days.			
Discussion Penetration testing of physical access points can provide information on critical vulnerabilities in the operating environments of organizational systems. Such information can be used to correct weaknesses or deficiencies in physical controls that are necessary to protect organizational systems.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls CA-2, PE-3;		**Reference Policy** See CA-8;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CA-09**	**Control Name** **Internal System Connections**	**Priority** **P2**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement (a) Authorize internal connections of system components or classes of components (defined in the applicable system security and privacy plan) to the system; (b) Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated; (c) Terminate internal system connections upon issuance of an order by the CMS CIO, CISO, or Senior Official for Privacy (SOP) and when such internal system connections no longer support CMS missions or business functions; and (d) Review the continued need for each internal connection at least every three hundred sixty-five (365) days. .			
Discussion Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system). Intra-system connections include connections with mobile devices, notebook and desktop computers, workstations, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal system connection, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability; or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.			
Implementation Standard High & Moderate: Std.1 - The security and privacy plan will identify the types of personally owned equipment that may be internally connected with organizational systems and networks: (a) Compliant with CMS and HHS policies on use of personally owned equipment; (b) Use of Bluetooth interconnections is disallowed without explicit approval of the Authorizing Official (AO).			
Control Review Frequency		**Assessment Frequency**	

Annually (365 Days)	Annually (365 Days)

Related Controls
AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4, SI-12;
(Redacted Privacy Controls: UL-1, UL-2)
	Reference Policy
	Code: 5 U.S.C. §552a(b) and (e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	HHS: Information Systems Security and Privacy Policy (IS2P) 2014;
	HIPAA: 45 C.F.R. §164.312(a)(1), 45 C.F.R. §164.312(d), 45 C.F.R. §164.312(e)(1);
	NISTIR: 8023;
	NIST SP: 800-124;
	OMB Circular: A-130 7.g. and 8.b(3)(b);

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): Include privacy requirements in the Information Connection Document (or equivalent such as an Interconnection Security Agreement or an Authority to Connect package), specifically addressing the collection authority, compatibility of purpose for use, and need for recipient of information to achieve specific business purpose. Documentation must also address responsibilities of the receiving system for protecting personally identifiable information (PII).	
Privacy Implementation Standards Systems processing, storing, or transmitting PII (to include PHI): High & Moderate: PRIV.1 - The internal use of PII on internal system connections must be used for an official government purpose only. The officers and employees of the CMS Business/System must have a need for the PII in the performance of their official duties.	
HVA Control Statement (a) Document and authorize internal connections between the HVA environment and other organizational systems (including support systems). CMS may choose to develop a streamlined version of a typical ISA/MOU to be used for internal connections. (b) Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated; (c) Terminate internal system connections upon issuance of an order by the CMS CIO, CISO, or Senior Official for Privacy (SOP) and when such internal system connections no longer support CMS missions or business functions; and (d) Review the continued need for each internal connection at least every three hundred sixty-five (365) days.	
HVA Discussion Organizations should identify the connections between the HVA and other system components within the HVA boundary to understand the critical dependencies of the HVA. In conjunction with CA-6(1), the Overlay specifies that these interconnections are to be documented and authorized in accordance with the Joint Authorization methodology.	
HVA Implementation Standard Systems designated as HVA: High & Moderate: HVA.1 - Document and authorize internal connections between the HVA environment and other organizational systems (including support systems) using Interconnection Security Agreements (ISA) and Memorandum of Understanding (MOU).	

Control Number **CA-09(01)**	**Control Name** **Compliance Checks**	**Priority** **P3**	**CMS Baseline** **Above Baseline**
Control Statement Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.			
Discussion Compliance checks include verification of the relevant baseline configuration.			
Implementation Standard			
Control Review Frequency		**Assessment Frequency**	

Not Specified	Three (3) Years

Related Controls
CM-6;
	Reference Policy
	Code: 5 U.S.C. §552a(b) and (e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	HIPAA: 45 C.F.R.§164.312(a)(1), 45 C.F.R. §164.308(a)(8), 45 C.F.R. §164.308(a)(1)(i), 45 C.F.R. §164.306(a), 45 C.F.R.§164.312(d), 45 C.F.R. §164.312(e)(1);
	OMB Circular: A-130 7.g. and 8.b(3)(b);

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): Compliance checks may include an assessment, prior to initial connection, of specific components, e.g., printers, based on sensitivity of personally identifiable information (PII) processed by that component. Any change to the components' security posture would require a re-verification of the configuration settings.	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Configuration Management

Control Number	Control Name	Priority	CMS Baseline
CM-01	Policy and Procedures	P1	Low Moderate High

Control Statement

(a) Develop, document, and disseminate to applicable personnel and roles:

1. CMS Enterprise-level configuration management policy that:
   a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the configuration management policy and procedures; and

(c) Review and update the current configuration management:

1. Policy at least every three (3) years and following defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures at least every three (3) years and following defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

This control addresses policy and procedures for the controls in the CM family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise level configuration management policy within this ARS, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures.)

Implementation Standard

High, Moderate & Low:

Std.1 - The configuration management process and procedure is documented to define configuration items at the system and component level (e.g., hardware, software, workstation); monitor configurations; and track and approve changes prior to implementation, including, but not limited to, flaw remediation, security patches, and emergency changes (e.g., unscheduled changes such as mitigating newly discovered security vulnerabilities, system crashes, replacement of critical hardware components).

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years

Related Controls	Reference Policy

PM-9, PS-8, SA-8, SI-12;	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, AS-3, CM-1, CM-3.1.1, CM-3.1.2, CM-3.1.3, CM-3.1.4, CM-3.1.5, CM-3.1.6, CM-3.1.7, CM-3.1.8, CM-3.1.9, SM-1, SM-3;
	NIST SP: 800-12, 800-30, 800-39, 800-100;
	OMB Circular: A-130;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
The configuration management policy and procedures should address the strategy for including applicable privacy requirements and controls in the systems. As such, updates to the configuration management policy and procedures must also address changes in federal privacy laws and policy requirements. Since CMS requires at least every three-year review of the configuration management policy and procedures, the statute driven requirement to review the privacy policy and procedures every two years will be met.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
High & Moderate:
PRIV.1 - Monitor for changes to applicable privacy laws, regulations, and overarching policy that affect configuration management policies no less often than once every 365 days to ensure the CMS and Mission/Business/System configuration management policies remains effective.
PRIV.2 - Ensure configuration management policies support privacy to the greatest extent feasible throughout the system's life cycle.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **CM-02**	**Control Name** **Baseline Configuration**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**

Control Statement

(a) Develop, document, and maintain under configuration control, a current baseline configuration of the system; and
(b) Review and update the baseline configuration of the system:
1. At least every 180 days for High systems or 365 days for Moderate systems;
2. When required due to major system changes/upgrades, critical security patches (as defined by the Federal Government, CMS, or vendor), and emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware components); and
3. When system components are installed or upgraded;

Discussion

Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture.

Implementation Standard

High, Moderate & Low:
Std.1 – Baseline configurations will be distilled from government, industry, and vendor standards and best practices.
Std.2 – Baseline configurations must include security updates.
Std.3 – Baseline configuration requirements apply to all systems, devices, appliances, and applications.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Annually (365 Days)

Related Controls	**Reference Policy**

AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18;	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-3, CM-2, CM-2.1.1, CM-2.1.2, CM-2.1.3;
	HHS: End of Life Operating Systems and Applications Policy;

	NIST SP: 800-128, 800-124;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a) Develop, document, and maintain under configuration control, a current baseline configuration of the HVA system; and

(b) Review and update the baseline configuration of the HVA system:

1. At least every 180 days for High systems or 365 days for Moderate systems;
2. When required due to major system changes/upgrades, critical security patches (as defined by the Federal Government, CMS, or vendor), and emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware components); and
3. When system components are installed or upgraded;
4. As an integral part of system component installations and upgrades.

HVA Discussion

Baseline configurations for the HVA and HVA components include connectivity, operational, and communications aspects. Baseline configurations are documented, formally reviewed and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of the HVA may or may not reflect the current enterprise architecture (EA), depending on the nature of the HVA and its function(s) (i.e. mainframe-based HVAs or other legacy and/or specialized system).

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
CM-02(02)	**Automation Support for Accuracy and Currency**	**P1**	**Moderate** **High** **HVA**

Control Statement

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms. (Automation support examples include hardware asset management systems, software asset management systems, and centralized configuration management software)

Discussion

Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, and firmware inventory tools, and network management tools. Automated tools can be used at the organization level, mission/business process level or system level on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels. Automation support for accuracy and currency can be satisfied by the implementation of CM-8(2) for organizations that combine system component inventory and baseline configuration activities.

Implementation Standard

Std. 1 Configure the system architecture to allow automated hardware and software mechanisms provided by Continuous Diagnostics and Mitigation (CDM) to scan the system
Std.2 Configure the access controls, as needed, to allow automation support to have access to the information that it needs
Std. 3 Run automated mechanisms to gather hardware and software configurations as part of the Continuous Monitoring Program

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)
Related Controls	**Reference Policy**

CM-7, IA-3, RA-5;	FedRAMP: Rev. 4 Baseline;
	OMB Memo: M-14-03, M-15-01;
	NIST SP: 800-37, 800-100, 800-128;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **CM-02(03)**	**Control Name** **Retention of Previous Configurations**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Retain previous (older) versions of baseline configurations of the system as deemed necessary to support rollback.			
Discussion Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, and configuration records.			
Implementation Standard High & Moderate: Std.1 – Following baseline configuration updates, no less than one (1) older baseline configuration must be maintained (e.g., for emergency rollback).			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
None;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		NIST SP: 800-34, 800-100, 800-128;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CM-02(06)**	**Control Name** **Development and Test Environments**	**Priority** **P3**	**CMS Baseline** **Above Baseline**
Control Statement Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.			
Discussion Establishing separate baseline configurations for development, testing, and operational environments protects systems from unplanned or unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, the management of operational configurations typically emphasizes the need for stability, while the management of development or test configurations requires greater flexibility. Configurations in the test environment mirror configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. Separate baseline configurations does not necessarily require separate physical environments.			
Implementation Standard High: Std.1 - The organization must provide separated environments where execution and analysis of data may present an enhanced risk to the system.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls CM-4, SC-3, SC-7;		**Reference Policy** See CM-2;	
Privacy Discussion			

Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **CM-02(07)**	**Control Name** **Configure Systems and Components for High-Risk Areas**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement (a) Issue systems, system components, or devices (e.g., CMS government-furnished laptops, mobile devices, equipment) with stringent configurations (e.g., FIPS 140-2 compliant encryption) to individuals traveling to locations that the organization deems to be of significant risk; and (b) Apply security safeguards to systems, system components, or devices (e.g., detailed inspection and examination of the device (GFE) for physical tampering, purging or reimaging the hard disk drive/removable media) when the individuals return from travel.
Discussion When it is known that systems, system components or devices (e.g., notebook computers, mobile devices) will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the MP (Media Protection) family.
Implementation Standard

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
MP-4, MP-5;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	NIST SP: 800-128;

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **CM-03**	**Control Name** **Configuration Change Control**	**Priority** **P1**	**CMS Baseline** **Moderate** **High** **HVA**

Control Statement (a) Determine and document the types of changes to the system that are configuration-controlled; (b) Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; (c) Document configuration change decisions associated with the system; (d) Implement approved configuration-controlled changes to the system;

(e) Retain records of configuration-controlled changes to the system for no less than twelve (12) months after the change
(f) Monitor and review activities associated with configuration-controlled changes to the system; and
(g) Coordinate and provide oversight for configuration change control activities through change request forms which must be approved by an organizational and/or CMS Change Control Board that convenes frequently enough to accommodate proposed change requests, and other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff.

Discussion

Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations and configuration items of systems; changes to operational procedures; changes to configuration settings for system components; unscheduled or unauthorized changes; and changes to remediate vulnerabilities. Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes. For changes impacting privacy risk, the Senior Agency Official for Privacy (SAOP) updates privacy impact assessments and system of records notices. For new systems or major upgrades, organizations consider including representatives from the development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10.

Implementation Standard

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-7, RA-8, SA-8, SA-10, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SI-12, SR-11;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-3, CM-1.1.1, CM-3, CM-6;
	HIPAA: 45 C.F.R.§164.312(a)(2)(iv), 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.312(e)(2)(ii);
	NISTIR 8062;
	NIST SP: 800-124, 800-128;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a) Determine and document the types of changes to the system that are configuration-controlled;
(b) Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
(c) Document configuration change decisions associated with the system;
(d) Implement approved configuration-controlled changes to the system;
(e) Retain records of configuration-controlled changes to the system for a minimum of three (3) years after the change;
(f) Monitor and review activities associated with configuration-controlled changes to the system; and
(g) Coordinate and provide oversight for configuration change control activities through change request forms which must be approved by an organizational and/or CMS Change Control Board that convenes frequently enough to accommodate proposed change requests, and other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff.

HVA Discussion

Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations and configuration items of systems; changes to operational procedures; changes to configuration settings for system components; unscheduled or unauthorized changes; and changes to remediate vulnerabilities. Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes. For changes impacting privacy risk, the Senior Agency Official for Privacy (SAOP) updates privacy impact assessments and system of records notices. For new systems or major upgrades, organizations consider including representatives from the development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10.

HVA Implementation Standard

Control Number **CM-03(01)**	**Control Name** **Automated Documentation, Notification, and Prohibition of Changes**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Use automated mechanisms to: (a) Document proposed changes to the system; (b) Notify designated approval authorities (defined in the applicable security and privacy plan) of proposed changes to the system and request change approval; (c) Highlight proposed changes to the system that have not been approved or disapproved within a time period specified by the system change management process (defined in the applicable security and privacy plan); (d) Prohibit changes to the system until designated approvals are received; (e) Document all changes to the system; and (f) Notify applicable personnel or stakeholders when approved changes to the system are completed. A list of applicable personnel or stakeholders must include, but not limited to the following: - Change Control Board (CCB); - Configuration Management Executive; - Chief Risk Officer (CRO); - Cyber Risk Advisor (CRA); - ISSO; - Program Manager; - Data Guardian; - Information System Owner (ISO); and - Information System Administrator.			
Discussion			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls None;		**Reference Policy** See CM-3;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CM-03(02)**	**Control Name** **Testing, Validation, and Documentation of Changes**	**Priority** **P1**	**CMS Baseline** **Moderate** **High** **HVA**
Control Statement Test, validate, and document changes to the system before finalizing the implementation of the changes on the operational system.			
Discussion			

Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with system operations supporting organizational missions and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures, system security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).

- To better secure IT infrastructure, configuration management procedure should include use of a security configuration checklist (sometimes called a lockdown, hardening guide, or benchmark) to help configure systems to an operating environment.
- Authorization (authorization to operate given identified risk and security and privacy controls) is maintained when proposed or actual changes to the system, and their suspected impact on the security and privacy posture of the system, are documented and continuously monitored for compliance.
- Configuration Management process includes the following steps:
  1. Identify change;
  2. Evaluate change request;
  3. Approve, Deny or Defer implementation of the change;
  4. Implement the approved change; and
  5. Continuously monitor change for acceptable operation.

Implementation Standard

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Annually (365 Days)
Related Controls	**Reference Policy**
FISCAM: CM-3.1.1, CM-3.1.2, CM-3.1.3, CM-3.1.4, CM-3.1.5, CM-3.1.6, CM-3.1.7, CM-3.1.8, CM-3.1.9;	NIST SP: 800-100

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

Test, validate, and document configuration changes to the HVA system before finalizing the implementation of the changes.

HVA Discussion

Changes to the HVA include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Individuals or groups conducting tests understand security and privacy policies and procedures, HVA security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. An operational HVA may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If the HVA must be taken off-line for testing, the tests should be scheduled to occur during planned system outages, when possible. If the testing cannot be conducted on an operational HVA, organizations should annotate an acceptance of risk in the HVA system security plan and/or consider employing compensating controls, such as CM-2 and CM-3(7).

HVA Implementation Standard

Std. 1 Ensure testing does not interfere with HVA operations supporting organizational missions and business functions

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CM-03(04)	**Security and Privacy Representatives**		**Moderate** **High**

Control Statement

Require CMS-defined security and privacy representatives to be members of the CMS-defined configuration change control element.

Discussion

Information security and privacy representatives include system security officers, senior agency information security officers, senior agency officials for privacy, or system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect

the security and privacy posture of systems. The configuration change control element referred to in the second organization-defined parameter reflects the change control elements defined by organizations in CM-3g.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls None	**Reference Policy**
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
CM-03(06)	**Cryptography Management**	**P3**	**High**

Control Statement Ensure that cryptographic mechanisms used to provide the following controls (security and privacy safeguards) are under configuration management (defined in the applicable security and privacy plan)	
Discussion The controls referenced in the control enhancement refer to security or privacy controls from the control catalog. Regardless of the cryptographic mechanisms employed, processes and procedures are in place to manage those mechanisms. For example, if system components use certificates for identification and authentication, a process is implemented to address the expiration of those certificates.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls SC-8, SC-12, SC-13, SC-28;	**Reference Policy** See CM-3;
Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): When cryptographic mechanisms are used to safeguard personally identifiable information (PII) (e.g. encrypting PII), management processes and procedures must be in place to manage those mechanisms (e.g. access to sensitive PII, key management, expiration of certificates) Discussion for systems processing, storing, or transmitting PHI: When cryptographic mechanisms are used to safeguard protected health information (PHI) (e.g. encrypting PHI), management processes and procedures must be in place to manage those mechanisms (e.g. access to PHI, key management, expiration of certificates)	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
CM-03(07)	**Review System Changes**		**HVA**

Control Statement Review changes to the system: (a) At least once a week [every seven (7) days] or;

(b) When unauthorized changes have occurred	
Discussion Indications that warrant review of changes to the system and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process or continuous monitoring process.	
Implementation Standard Moderate & High: Std.1 - The system configuration must be continuously monitored as a supplemental information source for the review processes. Std.2 - System changes must be verified to meet system mission and user requirements.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls AU-6, AU-7, CM-3;	**Reference Policy** NIST SP: 800-37, 800-100
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Review changes to the HVA system: (a) At least once a week [every seven (7) days] or; (b) When unauthorized changes or unexpected levels of system performance are indicated	
HVA Discussion Indications that warrant review of changes to the system and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process or continuous monitoring process.	
HVA Implementation Standard HVA.1 – Review and monitor HVA system configuration regularly to determine unauthorized changes (e.g. unscheduled or unplanned system restarts).	

Control Number **CM-04**	**Control Name** **Impact Analyses**	**Priority** **P2**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.			
Discussion Organizational personnel with security or privacy responsibilities conduct impact analyses. Individuals conducting impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the security or privacy ramifications. Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing with stakeholders the impact of changes on organizational supply chain partners; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses also include risk assessments to understand the impact of the changes and to determine if additional controls are required.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
CA-2, CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, SA-4, SA-5, SA-8, SA-10, SI-2;
		Reference Policy
		Statute: E-Government Act of 2002 (Pub. L. No. 107-347), §208;
		FedRAMP: Rev. 4 Baseline;	

<table>
<tr><td>(Redacted Privacy Controls: AR-2)</td><td>FISCAM: AS-3, AS-3.5.1, CM-3.1.1, CM-3.1.2, CM-3.1.3, CM-3.1.4, CM-3.1.5, CM-3.1.6, CM-3.1.7, CM-3.1.8, CM-3.1.9, CM-4;
HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(A), 45 C.F.R. §164.308(a)(1)(ii)(B), 45 C.F.R. §164.308(a)(8);
NIST SP: 800-128;
OMB Memo: M-03-22;</td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b>
Discussion for systems processing, storing, or transmitting PII (to include PHI):
When analyzing changes to the system, the impacts to privacy are also considered. If necessary, conduct a privacy impact assessment.</td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b>
Analyze changes to the HVA system to determine potential security and privacy impacts prior to change implementation.</td></tr>
<tr><td colspan="2"><b>HVA Discussion</b>
Organizational personnel with security or privacy responsibilities conduct impact analyses. Individuals conducting impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the security or privacy ramifications. Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing with stakeholders the impact of changes on organizational supply chain partners; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses also include risk assessments to understand the impact of the changes and to determine if additional controls are required.</td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>CM-04(01)</b></td><td><b>Control Name</b>
<b>Separate Test Environments</b></td><td><b>Priority</b>
<b>P2</b></td><td><b>CMS Baseline</b>
<b>High</b>
<b>HVA</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
A separate test environment requires an environment that is physically or logically separate and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and that information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not implemented, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines).</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
SA-11, SA-15(9), SC-3, SC-7;
(Redacted Privacy Controls: AP-2, AR-3, DM-2, DM-3, UL-1)</td><td colspan="2"><b>Reference Policy</b>
Code: 5 U.S.C. §552a(e)(10);
Statute: Privacy Act of 1974 (P.L. 93-579);
OMB Circular: A-130 7.g.</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b>
Discussion for systems processing, storing, or transmitting PII (to include PHI):
If personally identifiable information (PII) is used in the test environment, then the same controls required for systems containing PII must be applied to the test environment. Simulated PII information should be used to the maximum extent practicable when testing system functionality.</td></tr>
</table>

Privacy Implementation Standards
HVA Control Statement Analyze (proposed) changes to the HVA system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.
HVA Discussion A separate test environment requires an environment that is physically or logically separate and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and that information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments cannot be implemented, organizations should determine the strength of the mechanism required when implementing logical separation. HVA system owner and HVA system component tester roles and duties should be separate, as outlined in control AC-5. Appropriate separation of duties supports valid testing of the HVA, helps to protect the integrity of the HVA, and reduces potential conflicts of interest between testers, operators, developers, or individuals that directly interact with the HVA or its components prior to production environment implementation.
HVA Implementation Standard Std. 1 Analyze HVAs in a separate test environment for flaws, weaknesses, incompatibilities, or intentional alterations.

<table>
<tr><td><b>Control Number</b>
<b>CM-04(02)</b></td><td><b>Control Name</b>
<b>Verification of Controls</b></td><td><b>Priority</b>
<b>P3</b></td><td><b>CMS Baseline</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Implementation in this context refers to installing changed code in the operational system that may have an impact on security or privacy controls. In general, the goal is to verify that system changes do not adversely impact security or privacy functions and the system’s ability to meet mission requirements.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High & Moderate:
Std.1 - Any system, including development and test, that contains and/or processes sensitive information (e.g., personally identifiable information [PII]) must verify security functions as per this control.
Std.2 - The system’s security functions must be continuously monitored and evaluated to ensure they are operating as intended and changes do not have an adverse effect on system performance.
Std.3 - Actions must be taken to verify that the provisioned security function implementation being assessed and/or monitored meets security function requirements, and is an approved system configuration.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
SA-11, SC-3, SI-6;</td><td colspan="2"><b>Reference Policy</b>
Code: 5 U.S.C. §552a(e)(10);
Statute: Privacy Act of 1974 (P.L. 93-579);
HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(D), 45 C.F.R. §164.308(a)(8), 45 C.F.R. §164.316(b)(2)(iii);
OMB Circular: A-130 7.g.;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b>
Discussion for systems processing, storing, or transmitting PII (to include PHI):
If a system change is made, verification of privacy overlay security control function is required to ensure continued compliance with privacy-related statutes and regulations.</td></tr>
</table>

Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **CM-05**	**Control Name** **Access Restrictions for Change**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.			
Discussion Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system, can potentially have significant effects on the security of the systems or individual privacy. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes. Access restrictions include physical and logical access controls (see AC-3 and PE-3), software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into systems), and change windows (i.e., changes occur only during specified times).			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		FISCAM: AS-3, AS-3.1.1, CM-4;
		NIST SP: 800-100;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CM-05(01)**	**Control Name** **Automated Access Enforcement and Audit Records**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement (a) Enforce access restrictions using automated mechanisms; and (b) Automatically generate audit records of the enforcement actions.			
Discussion Organizations log access records associated with applying configuration changes to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
AU-2, AU-6, AU-7, AU-12, CM-3, CM-6, CM-11, SI-12;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		NIST SP: 800-100;	

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **CM-05(05)**	**Control Name** **Privilege Limitation for Production and Operation**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement (a) Limit privileges to change system components and system-related information within a production or operational environment; and (b) Review and reevaluate privileges CMS-defined frequency].			
Discussion : In many organizations, systems support multiple mission and business functions. Limiting privileges to change system components with respect to operational systems is necessary because changes to a system component may have far-reaching effects on mission and business processes supported by the system. The relationships between systems and mission/business processes are, in some cases, unknown to developers. System-related information includes operational procedures.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls AC-2		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CM-05(06)**	**Control Name** **Limit Library Privileges**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Limit privileges to change software resident within software libraries.			
Discussion Software libraries include privileged programs.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls AC-2		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number	Control Name	Priority	CMS Baseline
CM-06	**Configuration Settings**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

(a) Establish and document configuration settings for components employed within the system using the latest security baseline configurations established by the HHS, U.S. Government Configuration Baselines (USGCB), and the National Checklist Program (NCP) defined by NIST SP 800-70 Rev. 2 (refer to Implementation Standard 1 for specifics) that reflect the most restrictive mode consistent with operational requirements;
(b) Implement the configuration settings;
(c) Identify, document, and approve any deviations from established configuration settings for system components based on explicit operational requirements (defined in the applicable system security and privacy plan); and
(d) Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Discussion

Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Security parameters are parameters impacting the security posture of systems, including the parameters required to satisfy other security control requirements. Security parameters include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system.

Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products and platforms as well as instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors.

Implementation of a common secure configuration may be mandated at the organization level, mission/business process level, or system level, or may be mandated at a higher level, including by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline (USGCB) and security technical implementation guides (STIGs), which affect the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.

Implementation Standard

High, Moderate & Low:
Std.1 - Use of HHS and CMS approved Operating System (OS)
(a) HHS-specific minimum security configurations must be used for the following OS and Applications:
1. HHS approved USGCB Windows Standards (e.g., Microsoft supported versions only); and
2. Blackberry Server - Websense.
(b) For all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing security configuration guidelines is:
1. USGCB;
2. NIST NCP; Tier IV, then Tier III, Tier II, and Tier I, in descending order;
3. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG);
4. National Security Agency (NSA) STIGs;
5. If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group (such as The Center for Internet Security [CIS]) checklists.
6. In situations where no guidance exists, coordinate with CMS for guidance. CMS must collaborate within CMS and the HHS Cybersecurity Program, and other organizations through the HHS Continuous Monitoring and Risk Scoring (CMRS) working group to:
- Establish baseline configurations and communicate industry and vendor best practices; and

- Ensure deployed configurations are supported for security updates.

7. All deviations from existing USGCB, NCP, DISA and/or NSA configurations must be documented.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-3, CM-2, CM-2.1.1, CM-2.1.2, CM-2.1.3;
	HHS: End of Life Operating Systems and Applications Policy;
	NIST SP: 800-70, 800-128;
	OMB Memo: M-07-18, M-08-22;
	Web: HYPERLINK "https://nvd.nist.gov/ncp/repository" , HYPERLINK "https://www.nsa.gov" , HYPERLINK "https://nvd.nist.gov" ;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PHI:

HIPAA requires CMS Businesses/Systems follow specific procedures for de-identification and to implement policies and procedures to address the final disposition of PHI (such as in a NARA repository) and/or the hardware or electronic media on which it is stored.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Where feasible, configure systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under a NARA-approved Records Schedule.

HVA Control Statement

(a) Establish and document configuration settings for HVA components employed within the system using the latest security baseline configurations established by the HHS, U.S. Government Configuration Baselines (USGCB), and the National Checklist Program (NCP) defined by NIST SP 800-70 Rev. 2 that reflect the most restrictive mode consistent with operational requirements. track deviations from established baselines for the HVA and components that comprise the HVA;

(b) Implement the configuration settings;

(c) Identify, document, and approve any deviations from established configuration settings for system components based on explicit operational requirements (defined in the applicable system security and privacy plan); and

(d) Monitor and control changes to the configuration settings in accordance with organizational policies and procedures."

HVA Discussion

Configuration settings apply to HVA systems and the HVA components. Changes to those configuration settings are monitored, tracked, and controlled by the organization.

HVA Implementation Standard

•Ensure the HVA baseline configurations enforce secure authentication;

•Ensure the HVA does not allow for a common local administrator password on all the workstations, servers, and systems;

•Ensure default configurations and passwords of HVA commercial and government-off-the-shelf (COTS/GOTS) products are modified and not left as default;

•Verify the default configurations are not reverted to each time the HVA

•COTS packages are updated or upgraded

Control Number	Control Name	Priority	CMS Baseline
CM-06(01)	**Automated Management, Application, and Verification**	**P1**	**High**

Control Statement

Manage, apply, and verify configuration settings for system components as defined in the HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications.

Discussion

Automated tools [e.g., security information and event management (SIEM) tools or enterprise security monitoring tools] can improve the accuracy, consistency, and availability of configuration settings information. Automation can also provide data aggregation and data correlation capabilities; alerting mechanisms; and dashboards to support risk-based decision making within the organization.	
Implementation Standard High: Std.1 - The system must be continuously monitored and assessed to ensure that it is operating as intended and that changes do not have an adverse effect on system performance. Std.2 - Automated central management mechanisms for systems must be verified to meet system mission and user requirements.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
CA-7, CM-4;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	NIST SP: 800-37, 800-100;
	HHS: Minimum Security Configuration Standards for Departmental Operating Systems and Applications;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CM-06(02)	**Respond to Unauthorized Changes**	**P1**	**High** **HVA**

Control Statement Take the following actions in response to unauthorized changes to configuration settings of systems and system components (e.g., authorization, auditing, processing types, baseline configurations, system libraries, log files, executables) in the following ways: (a) Alert responsible personnel or role (defined in the applicable system security and privacy plan); (b) Restore to approved configuration; and (c) Halt system processing as warranted.	
Discussion Responses to unauthorized changes to configuration settings include alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected system processing.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
IR-4, IR-6, SI-7;
	Reference Policy
	NIST SP: 800-37, 800-39, 800-137;
	OMB Memo: M-14-03, M-15-01, M-16-04, M-19-03;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Respond to unauthorized changes to configuration settings of systems and system components (e.g., authorization, auditing, processing types, baseline configurations, system libraries, log files, executables) and authorized HVA configurations in accordance with the organizational configuration management policies and procedures in the following ways:	

(a) Alert responsible personnel or role (defined in the applicable system security and privacy plan);
(b) Restore to approved configuration; and
(c) Halt system processing as warranted.

HVA Discussion

Organizations should cross reference detected changes with change control documentation to determine if the change was preauthorized. Organizations should be prepared for action and ensure processes are documented on detection of unauthorized changes to systems. Organizations should also employ safeguards to respond to and remediate unauthorized changes to configuration settings.

HVA Implementation Standard

Std. 1 Employ safeguards to respond to and remediate unauthorized changes to configuration settings
Std. 2 Report all unauthorized changes in accordance with the CMS incident response processes.

Control Number	Control Name	Priority	CMS Baseline
CM-07	**Least Functionality**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

(a) Configure the system to provide only essential capabilities (defined in applicable security/privacy plans) and
(b) Prohibit or restrict the use of high-risk system services, functions, ports, network protocols, and capabilities (e.g., Telnet, FTP, etc.) across network boundaries that are not explicitly required for system or application functionality;

Discussion

Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA-8, SC-2, and SC-3).
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Implementation Standard

High, Moderate & Low:
Std.1 - Automated configuration review results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Configuration review information sources include systems, appliances, devices, services, and applications (including databases).
(c) CCIC directed configuration review information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.
Std.3 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational configuration status and posture information.

Control Review Frequency	Assessment Frequency

Annually (365 Days)	Annually (365 Days)

Related Controls
AC-3, AC-4, AC-6, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC-2, SC-3, SC-7, SC-37, SI-4;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-3, AS-2;
	NIST SP: 800-37, 800-39, 800-137;
	OMB Memo: M-14-03, M-15-01, M-16-04, M-19-03;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a) Configure the system to provide only essential capabilities; and

(b) Prohibit or restrict the use of high-risk system services, functions, ports, network protocols, and capabilities (e.g., Telnet, FTP, etc.) across network boundaries that are not explicitly required for system or application functionality;

(c) A list of specifically needed system services, ports, and network protocols must be maintained and documented in the applicable security and privacy plan; all others will be disabled

HVA Discussion

Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA-8, SC-2, and SC-3).

Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

HVA Implementation Standard

High, Moderate & Low:

Std.1 - Automated configuration review results must be searchable by the CCIC:

(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;

(b) Configuration review information sources include systems, appliances, devices, services, and applications (including databases).

(c) CCIC directed configuration review information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.

Std.2 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Std.3 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational configuration status and posture information.

Control Number	Control Name	Priority	CMS Baseline
CM-07(01)	**Periodic Review**	**P1**	**Moderate** **High** **HVA**

Control Statement

(a) Review the system upon encountering a significant risk, or at least every thirty (30) days to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

(b) Disable or remove functions, ports, protocols, software, and services within the information system deemed to be unnecessary and/or nonsecure.

Discussion

Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination. Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.

Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Implementation Standard

High & Moderate:

Std.1 - Periodic configuration review results that are generated by automated tools must be searchable by the CCIC:

(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;

(b) Configuration review information sources include systems, appliances, devices, services, and applications (including databases); and

(c) CCIC directed configuration automated periodic review information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.

Std.2 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Control Review Frequency	**Assessment Frequency**
Monthly	Annually (365 Days)

Related Controls
AC-18, CM-7, IA-2;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	NIST SP: 800-37, 800-39, 800-137;
	OMB Memo: M-14-03, M-15-01, M- 16-04, M-19-03;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a) Review the HVA system no less often than once every thirty (30) days to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

(b) Disable or remove functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure. That do not hinder or otherwise impede the organization’s ability to complete its mission essential function(s), as
performed by the HVA.

HVA Discussion

Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IP version [v] 4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can decide on the relative security of the function, port, protocol and/or service or base the security decision on the results of periodic reviews of other organizations. Unsecure protocols include Bluetooth, file transfer protocol, and peer-to-peer networking.

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CM-07(02)	**Prevent Program Execution**	**P1**	**Moderate** **High**

Control Statement

Prevent program execution in accordance with policies regarding authorized software use which include, but are not limited to the following:

(a) Software must be legally licensed;

(b) Software must be provisioned in approved configurations; and

(c) Users must be authorized for software program use.	
Discussion Prevention of program execution addresses organizational policies, rules of behavior, and/or access agreements restricting software usage and the terms and conditions imposed by the developer or manufacturer, including software licensing and copyrights. Restrictions include prohibiting auto-execute features; restricting roles allowed to approve program execution; program denylisting and allow listing; or restricting the number of program instances executed at the same time.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls CM-8, PM-5, PL-4, PS-6;	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **CM-07(05)**	**Control Name** **Authorized Software - Allow**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement (a) Identify software programs (defined in the applicable security and privacy plan) authorized to execute on the system ; (b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and (c) Review and update the list of authorized software programs no less often than every seventy-two (72) hours.			
Discussion The process used to identify specific software programs or entire categories of software programs that are authorized to execute on organizational systems is commonly referred to as allow listing. Software programs identified can be limited to specific versions or from a specific source. To facilitate comprehensive allow listing and increase the strength of protection for attacks that bypass application level allow listing, software programs may be decomposed into and monitored at different levels of detail. Software program levels of detail include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. The concept of allow listing may also be applied to user actions, ports, IP addresses, and media access control (MAC) addresses. Organizations consider verifying the integrity of allow -listed software programs using, cryptographic checksums, digital signatures, or hash functions. Verification of allow -listed software can occur either prior to execution or at system startup. allow listing of URLs for websites is addressed in CA-3(5) and SC-7. Control enhancement CM-7(5) is only required for systems categorized under FIPS-199 as HIGH. Implementation of allow listing is an option for all systems (e.g., to include any system categorized under FIPS-199 as MODERATE and LOW). If the system owner/business owner chooses to implement CM-7(5) on systems categorized under FIPS-199 as MODERATE and LOW, CM-7(4) does not have to be implemented. Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.			
Implementation Standard High: Std.1 - An automated software allow software tool must be implemented. Std.2 - Authorized software allow software tool results must be searchable by the CCIC: (a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; (b) Authorized software allow listing (and denylisting) information sources include systems, appliances, devices, services, and applications (including databases);			

(c) Authorized software allow listing information sources that do not support the exchange of information with the CCIC must be documented in the applicable risk assessment and security plan; and (d) CCIC directed unauthorized software/allow listing information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.	
Control Review Frequency Six (6) Months	**Assessment Frequency** Annually (365 Days)

Related Controls
CM-2, CM-6, CM-8, CM-10, PM-5, SA-10, SC-34, SI-7;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	NIST SP: 800-37, 800-39, 800-137;
	OMB Memo: M-14-03, M-15-01, M- 16-04, M-19-03;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **CM-07(09)**	**Control Name** **Prohibiting the Use of Unauthorized Software**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement (a) Identify hardware components authorized for system use (defined in system security and privacy plan) (b) Prohibit the use or connection of unauthorized hardware components; (c) Review and update the list of authorized hardware components every 180 days.			
Discussion Hardware components provide the foundation for organizational systems and the platform for the execution of authorized software programs. Managing the inventory of hardware components and controlling which hardware components are permitted to be installed or connected to organizational systems is essential in order to provide adequate security			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None		**Reference Policy** [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-167].	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CM-08**	**Control Name** **System Component Inventory**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement (a) Develop and document an inventory of system components that:			

1. Accurately reflects the system;
2. Includes all components within the system;
3. Does not include duplicate accounting of components or components assigned to any other system;
4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes the following information to achieve system component accountability:
   - Each component's unique identifier and/or serial number;
   - Information system of which the component is a part;
   - Type of information system component (e.g., server, desktop, application);
   - Manufacturer/model information;
   - Operating system type and version/service pack level;
   - Presence of virtual machines;
   - Application software version/license information;
   - Physical location (e.g., building/room number);
   - Logical location (e.g., IP address, position with the information system [IS] architecture);
   - Media access control (MAC) address;
   - Ownership;
   - Operational status;
   - Primary and secondary administrators; and
   - Primary user; and

(b) Review and update the system component inventory at least every 180 days.

Discussion

System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. The information necessary for effective accountability of system components includes system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Implementation Standard

High, Moderate & Low:

Std.1 - All Government-owned equipment (i.e., servers, workstations, laptops, and other IT components) used to process, store, or transmit CMS information display an asset tag with a unique identifying asset number.

Std.2 - IT components with an asset tag are tracked in an asset inventory database to include (at a minimum) name of component, location, asset identification, owner, and description of use.

Std.3 - Fully integrate inventory of system components with the organizational continuous monitoring capability (CM-7).

Std.4 - Automated asset inventory information tracking systems must:

(a) Transmit updates to CCIC no less often that once every 72 hours.

Std.5 - Automated component tracking and management tool results must be searchable by the CCIC:

(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;

(b) Authorized component information sources include systems, platforms, appliances, devices;

(c) Component information sources that do not support the exchange of information with the CCIC must be documented in the applicable risk assessment and security plan; and

(d) CCIC directed authorized component information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.

Std.6 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Std.7 - Provide timely responses, as defined by the CISO, to informational requests for organizational component status and posture information.

Std.8 - Create and maintain the inventory of high value assets associated with the system.
(a) The inventory must identify other FISMA systems from which controls are inherited.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Annually (365 Days)
Related Controls	**Reference Policy**

CM-2, CM-6, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PM-5, SA-4, SA-5, SI-2, SR-4;	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-3, CM-2, CM-2.1.1, CM-2.1.2, CM-2.1.3;
	HIPAA: 45 C.F.R. §164.310(d)(1), 45 C.F.R.§164.310(d)(2)(iii);
	NIST SP: 800-37, 800-39, 800-128, 800-137;
	OMB Memo: M-14-03, M-15-01, M-16-04, M-19-03;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a) Develop and document an inventory of system components that:
1. Accurately reflects the system;
2. Includes all components within the system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes the following information to achieve system component accountability:
   - Each component’s unique identifier and/or serial number;
   - Information system of which the component is a part;
   - Type of information system component (e.g., server, desktop, application);
   - Manufacturer/model information;
   - Operating system type and version/service pack level;
   - Presence of virtual machines;
   - Application software version/license information;
   - Physical location (e.g., building/room number);
   - Logical location (e.g., IP address, position with the information system [IS] architecture);
   - Media access control (MAC) address;
   - Ownership;
   - Operational status;
   - Primary and secondary administrators; and
   - Primary user; and

(b) Review and update the HVA system component inventory at least every 72 hours consistent with CISA CDM reporting requirements

HVA Discussion

Organizations may implement automated solutions to perform component inventory of the environment within the CISA CDM requirement timeframe.

HVA Implementation Standard

Std.1- Review and update HVA system component inventory at least every 72 hours consistent with CMS CDM reporting requirements.

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CM-08(01)	**Updates During Installation and Removal**	**P1**	**Moderate** **High**

Control Statement

Update the inventory of system components as part of component installations, removals, and system updates.

Discussion

Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated routinely as part of component installations or removals, or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented. System updates include hardware, software, and firmware components.

Implementation Standard

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls PM-16;	**Reference Policy** See CM-8;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PHI:

Identifying any changes or updates to system inventories allows CMS Businesses/Systems to accurately track the equipment on which their systems are run and to maintain an accurate inventory of hardware and software used to collect and manage PHI. Maintaining a current inventory supports accountability controls and may also support breach response efforts.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **CM-08(02)**	**Control Name** **Automated Maintenance**	**Priority** **P1**	**CMS Baseline** **High**

Control Statement

Maintain the currency, completeness, accuracy, and availability of the inventory of system components using automated mechanisms.

Discussion

Organizations maintain system inventories to the extent feasible. For example, virtual machines can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. Automated maintenance can be achieved by the implementation of CM-2(2) for organizations that combine system component inventory and baseline configuration activities.

Implementation Standard

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls SI-7;	**Reference Policy** OMB Memo: M-16-04, M-19-03;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **CM-08(03)**	**Control Name** **Automated Unauthorized Component Detection**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement

(a) Detect the presence of unauthorized hardware, software, and firmware components within the system no less often than weekly [every seven (7) days] using automated mechanisms; and

(b) Take the following actions when unauthorized components and/or provisioned configurations are detected:
- Disable access to the identified component;
- Disable the identified component’s network access;
- Isolate the identified component; and
- Notify responsible personnel or role (defined in applicable security and privacy plan)

Discussion

Automated unauthorized component detection is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented in systems or in separate system components. When acquiring and implementing automated mechanisms, organizations consider whether such mechanisms depend on the ability of the system component to support an agent or supplicant in order to be detected since some types of components do not have or cannot support agents (e.g., IoT devices). Isolation can be achieved, for example, by placing unauthorized system components in separate domains or subnets or quarantining such components. This type of component isolation is commonly referred to as sandboxing.

Implementation Standard

High & Moderate:

Std.1 - All components within the system authorization boundary must be monitored in compliance with information security continuous monitoring (ISCM) requirements.

Control Review Frequency Weekly	**Assessment Frequency** Annually (365 Days)
Related Controls AC-17, AC-18, AC-19, CA-7, SC-3, SC-39, SC-44, SI-3, SI-4, SI-7, RA-5;	**Reference Policy** FedRAMP: Rev. 4 Baseline;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **CM-08(04)**	**Control Name** **Accountability Information**	**Priority** **P1**	**CMS Baseline** **High**

Control Statement

Include in the system component inventory information, a means for identifying by position and role, individuals responsible and accountable for administering those components.

Discussion

Identifying individuals who are responsible and accountable for administering system components ensures that the assigned components are properly administered and that organizations can contact those individuals if some action is required, for example, the component is determined to be the source of a breach; the component needs to be recalled or replaced; or the component needs to be relocated.

Implementation Standard

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls None;	**Reference Policy** OMB Memo: M-16-04, M-19-03;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **CM-08(06)**	**Control Name** **Assessed Configurations and Approved Deviations**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.			
Discussion Assessed configurations and approved deviations focus on configuration settings established by organizations for system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls CM-2, CM-6		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CM-08(07)**	**Control Name** **Centralized Repository**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Provide a centralized repository for the inventory of system components.			
Discussion Organizations may implement centralized system component inventories that include components from all organizational systems. Centralized repositories of component inventories provide opportunities for efficiencies in accounting for organizational hardware, software, and firmware assets. Such repositories may also help organizations rapidly identify the location and responsible individuals of components that have been compromised, breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include system-specific information required for proper component accountability.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CM-09**	**Control Name** **Configuration Management Plan**	**Priority** **CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, SA-10, SI-12;**	**CMS Baseline** **Moderate** **High**
Control Statement Develop, document, and implement a configuration management plan for the system that: (a) Addresses roles, responsibilities, and configuration management processes and procedures;			

(b) Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; (c) Defines the configuration items for the system and places the configuration items under configuration management; (d) Is reviewed and approved by defined personnel or roles (e.g., CIO, CISO, SSO) (defined in applicable security and privacy plan); and (e) Protects the configuration management plan from unauthorized disclosure and modification.	
Discussion P1	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
FedRAMP: Rev. 4 Baseline;
NIST SP: 800-128;
	Reference Policy

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **CM-09(01)**	**Control Name** **Assignment of Responsibility**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.			
Discussion In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked with developing configuration management processes using personnel who are not directly involved in system development or system integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the system development and integration processes and configuration management processes to facilitate quality control and more effective oversight			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None		**Reference Policy** [SP 800-128].	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CM-10**	**Control Name** **Software Usage Restrictions**	**Priority** **P2**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement (a) Use software and associated documentation in accordance with contract agreements and copyright laws; (b) Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and			

(c) Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	
Discussion Software license tracking can be accomplished by manual or automated methods depending on organizational needs. A non-disclosure agreement is an example of a contract agreement.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls AC-17, AU-6, CM-7, CM-8, SC-7;	**Reference Policy** None;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CM-11	**User-Installed Software**	**P2**	**Low** **Moderate** **High**
Control Statement (a) Establish defined policies governing the installation of software by users on all GFE; (b) Enforce software installation policies through defined methods (defined in applicable security and privacy plan); and (c) Monitor policy compliance at least monthly [every thirty (30) days].			
Discussion If provided the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved “app stores.” Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization-developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.			
Implementation Standard High: Std.1 - Monitoring for user-installed software must comply with information security continuous monitoring (ISCM) requirements. Std.2 - allow listing applications must prevent un-authorized user-installed software. Moderate & Low: Std.1 - Monitoring for user-installed software must comply with information security continuous monitoring (ISCM) requirements.			
Control Review Frequency Monthly		**Assessment Frequency** Annually (365 Days)	
Related Controls		**Reference Policy** None;	

AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-7;	
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **CM-11(02)**	**Control Name** **Software Installation with Privileged Status**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Allow user installation of software only with explicit privileged status.			
Discussion Privileged status can be obtained, for example, by serving in the role of system administrator.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls AC-5, AC-6		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CM-12**	**Control Name** **Information Location**	**Priority**	**CMS Baseline** **Moderate** **High**
Control Statement (a) Identify and document the location of information and the specific system components on which the information is processed and stored; (b) Identify and document the users who have access to the system and system components where the information is processed and stored; and (c) Document changes to the location (i.e., system or system components) where the information is processed and stored.			
Discussion Information location addresses the need to understand where information is being processed and stored. Information location includes identifying where specific information types and associated information reside in the system components; and how information is being processed so that information flow can be understood, and adequate protection and policy management provided for such information and system components. The security category of the information is also a factor in determining the controls necessary to protect the information and the system component where the information resides (see FIPS 199). The location of the information and system components is also a factor in the architecture and design of the system (see SA-4, SA-8, SA-17).			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	
Related Controls		**Reference Policy**	

AC-2, AC-3, AC-4, AC-6, AC-23, CM-8, PM-5, RA-2, SA-4, SA-8, SA-17, SC-4, SC-16, SC-28, SI-4, SI-7;	FIPS 199;
	SP 800-60 v1;
	SP 800-60 v2.

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **CM-12(01)**	**Control Name** **Automated Tools to Support Information Location**	**Priority**	**CMS Baseline** **Moderate** **High**
Control Statement Use automated tools to identify information by information type on system components to ensure controls are in place to protect organizational information and individual privacy.			
Discussion The use of automated tools helps to increase the effectiveness and efficiency of the information location capability implemented within the system. Automation also helps organizations manage the data produced during information location activities and share such information organization-wide. The output of automated information location tools can be used to guide and inform system architecture and design decisions			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	
Related Controls None;		**Reference Policy** See CM-12;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CM-14**	**Control Name** **Signed Components**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Prevent the installation of network and server software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.			
Discussion Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input/output system updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures is a method of code authentication.			
Implementation Standard Std. 1 Apply the correct configuration that automatically stops firmware and software components from being installed without a digital signature. Std. 2 Ensure code that is taken from third party providers have a signature from the author.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls CM-7, SC-12, SC-13, SI-7		**Reference Policy** [IR 8062]	

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Contingency Planning

Control Number	Control Name	Priority	CMS Baseline
CP-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel and roles:

1. CMS Enterprise-level contingency planning policy that:
    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

(c) Review and update the current contingency planning:

1. Policy at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

This control addresses policy and procedures for the controls in the CP family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise level contingency planning policy within this ARS, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures.)

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

PM-9, PS-8, SI-12;	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-1, SM-3;
	HIPAA: 45 C.F.R. §164.308(a)(7)(i);
	NIST SP: 800-12, 800-34, 800-100, 800-50

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Contingency planning policy and procedures must take privacy-applicable requirements into account so that executing contingency measures does not result in avoidable privacy incidents and breaches.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Monitor for changes to applicable privacy laws, regulations, and overarching policy that affect contingency planning policies no less often than once every 365 days to ensure the CMS and Mission/Business/System contingency planning policies remains effective.
PRIV.2 - Ensure contingency planning policies support privacy to the greatest extent feasible throughout the system's life cycle.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
CP-02	**Contingency Plan**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

(a) Develop a contingency plan for the system that:
1. Identifies CMS essential missions and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
4. Addresses maintaining CMS essential missions and business functions despite a system disruption, compromise, or failure;
5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; and
6. Is reviewed and approved by CMS-defined personnel or role [e.g., Contingency Plan Coordinator (CPC), Business Owners];

(b) Distribute copies of the contingency plan to the ISSO, Business Owner, Contingency Plan Coordinator (CPC), and other stakeholders identified within the applicable system's contingency plan;
(c) Coordinate contingency planning activities with incident handling activities;
(d) Review the contingency plan for the system within every three hundred sixty-five (365) days;
(e) Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
(f) Communicate contingency plan changes to key contingency personnel or roles (e.g. the ISSO, System Owner, CPC, system administrator, database administrator) and other personnel/roles as appropriate; and
(g) Protect the contingency plan from unauthorized disclosure and modification.

Discussion

Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational missions and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
In addition to availability, contingency plans address other security-related events resulting in a reduction in mission effectiveness including malicious attacks that compromise the integrity of systems or the confidentiality of information. Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Organizations consider whether continuity of operations during an incident conflicts with the capability to automatically disable the system as specified in IR-4(5). Incident response planning is part of contingency planning for organizations and is addressed in the IR (Incident Response) family.

Implementation Standard

High, Moderate & Low:

Std.1 - The system must be continuously monitored [no less often than once every seventy-two (72) hours] and assessed to ensure that it is operating as intended and that changes do not have an adverse effect on system performance.
Std.2 - The organization must verify that the provisioned implementation being assessed and/or monitored meets users' needs and is an approved system configuration.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Annually (365 Days)

Related Controls	**Reference Policy**

AC-14, CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12;	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-3;
	HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.308(a)(7)(ii)(C), 45 C.F.R. §164.308(a)(7)(ii)(E), 45 C.F.R. §164.308(a)(7)(i)-(ii), 45 C.F.R. §164.310(a)(2)(i), 45 C.F.R. §164.312(a)(2)(ii);
	HSPD: HSPD 7 G(22)(i);
	NIST SP: 800-34;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
Contingency plans must take privacy-applicable requirements into account so that executing contingency measures does not result in avoidable privacy incidents and breaches.
Discussion for systems processing, storing, or transmitting PHI:
The contingency plan for systems containing PHI must include:
1) Data backup plan,
2) Disaster recovery plan,
3) Emergency mode operation plan, and
4) Emergency access procedures.
Additionally, the decision to include the following is dependent on a risk analysis to determine if or to what extent these should be included in the contingency plan:
1) Testing and revision procedures,
2) Applications and data criticality analysis, and
3) Contingency operations (i.e., procedures that allow facility access in support of restoration of lost data.

Privacy Implementation Standards

HVA Control Statement

(a) Develop a contingency plan for the HVA system that:
1. Identifies CMS essential missions and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
4. Addresses maintaining CMS essential missions and business functions despite a system disruption, compromise, or failure;
5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; and
6. Is reviewed and approved by CMS-defined personnel or role [e.g., Contingency Plan Coordinator (CPC), Business Owners];

(b) Distribute copies of the contingency plan to the ISSO, Business Owner, Contingency Plan Coordinator (CPC), and other stakeholders identified within the applicable system's contingency plan;
(c) Coordinate contingency planning activities with incident handling activities;
(d) Review the contingency plan for the system within every three hundred sixty-five (365) days;
(e) Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
(f) Communicate contingency plan changes to key contingency personnel or roles (e.g. the ISSO, System Owner, CPC, system administrator, database administrator) and other personnel/roles as appropriate;
(g) Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
(g) Protect the contingency plan from unauthorized disclosure and modification.

HVA Discussion

Contingency planning for systems to include HVAs is part of the organization’s overall program for achieving continuity of operations for organizational missions and business functions. Contingency planning addresses HVA restoration and implementation of alternative mission or business processes if the HVA is compromised or breached. Contingency planning should be considered throughout the HVA system development life cycle and is a fundamental part of the system design. Contingency plans reflect the degree of restoration required for organizational HVAs since not all systems need to fully recover to achieve the level of continuity of operations desired. HVA recovery objectives should reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
HVA Implementation Standard

Control Number **CP-02(01)**	**Control Name** **Coordinate with Related Plans**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Coordinate contingency plan development with organizational elements responsible for related plans.			
Discussion Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Cyber Incident Response Plans, and Occupant Emergency Plans.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
None;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		HSPD: HSPD 7 G(22)(i);
		NIST SP: 800-34;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CP-02(02)**	**Control Name** **Capacity Planning**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.			
Discussion Capacity planning is needed because different threats can result in a reduction of the available processing, telecommunications, and support services intended to support essential missions and business functions. Organizations anticipate degraded operations during contingency operations and factor the degradation into capacity planning. For capacity planning, environmental support refers to any environmental factor for which the organization determines that it needs to provide support in a contingency situation, even if in a degraded state. Such determinations are based on an organizational assessment of risk, system categorization (impact level), and organizational risk tolerance.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
PE-11, PE-12, PE-13, PE-14, PE-18, SC-5;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		HSPD: HSPD 7 G(22)(i);	

	NIST SP: 800-34;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
CP-02(03)	**Resume Missions and Business Functions**	**P3**	**Moderate** **High**

Control Statement

Plan for the resumption of all, essential missions and business functions within seventy two (72) hours of contingency plan activation, consistent with CMS COOP requirements.

Discussion

Organizations may choose to conduct contingency planning activities to resume missions and business functions as part of business continuity planning or as part of business impact analyses. Organizations prioritize the resumption of missions and business functions. The time-period for the resumption of missions and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)

Related Controls	Reference Policy
PE-12;	FedRAMP: Rev. 4 Baseline; NIST SP: 800-34

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
CP-02(05)	**Continue Missions and Business Functions**	**P1**	**High**

Control Statement

Plan for the continuance of essential missions and business functions [Primary Mission Essential Functions (PMEF)] with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

Discussion

Organizations may choose to conduct the contingency planning activities to continue missions and business functions as part of business continuity planning or as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)

Related Controls	Reference Policy

PE-12;	NIST SP: 800-34;
	45 C.F.R. §164.308(a)(7)(ii)(C);
	45 C.F.R. §164.312(a)(2)(ii)

Privacy Discussion

Discussion for systems processing, storing, or transmitting PHI: Pursuant to the emergency mode operations plan and emergency access procedure mandated under HIPAA, this control is required for both provision of emergency services (a mission critical business function), and for protection of the security of PHI while operating in emergency mode.
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **CP-02(06)**	**Control Name** **Alternate Processing and Storage Sites**	**Priority** **P1**	**CMS Baseline** **Above Baseline**
Control Statement Plan for the transfer of all essential mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.			
Discussion Organizations may choose to conduct contingency planning activities for alternate processing and storage sites as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls PE-12		**Reference Policy**	
Privacy Discussion Discussion for systems processing, storing, or transmitting PHI: Pursuant to the emergency mode operations plan and emergency access procedure mandated under HIPAA, this control is required for both provision of emergency services (a mission critical business function), and for protection of the security of PHI while operating in emergency mode.			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CP-02(07)**	**Control Name** **Coordinate with External Service Providers**	**Priority** **P1**	**CMS Baseline** **Above Baseline**
Control Statement Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.			
Discussion When the capability of an organization to carry out its mission and business functions is dependent on external service providers, developing a comprehensive and timely contingency plan may become more challenging. When mission and business functions are dependent on external service providers, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls SA-9		**Reference Policy**	
Privacy Discussion			

Discussion for systems processing, storing, or transmitting PHI: Pursuant to the emergency mode operations plan and emergency access procedure mandated under HIPAA, this control is required for both provision of emergency services (a mission critical business function), and for protection of the security of PHI while operating in emergency mode.
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **CP-02(08)**	**Control Name** **Identify Critical Assets**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Identify critical system assets supporting essential missions and business functions.			
Discussion Organizations may choose to identify critical assets as part of criticality analysis, business continuity planning, or business impact analyses. Organizations identify critical system assets so additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational missions and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include technical and operational aspects. Technical aspects include system components, information technology services, information technology products, and mechanisms. Operational aspects include procedures (manually executed operations) and personnel (individuals operating technical controls and/or executing manual procedures). Organizational program protection plans can assist in identifying critical assets. If critical assets are resident within or supported by external service providers, organizations consider implementing CP-2(7) as a control enhancement.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls CM-8, RA-9;		**Reference Policy** FedRAMP: Rev. 4 Baseline; NIST SP: 800-34, 800-60; 45 C.F.R. §164.308(a)(7)(ii) IR 8179	
Privacy Discussion Discussion for systems processing, storing, or transmitting PHI: This control addresses the HIPAA Security Rule requirement to assess the relative criticality of specific applications and data to facilitate a risk-based contingency plan. Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the CMS Business/System.			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CP-03**	**Control Name** **Contingency Training**	**Priority**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement			

<table>
<tr><td colspan="2">Provide contingency training to system users consistent with assigned roles and responsibilities:
(a) Within ninety (90) days of assuming a contingency role or responsibility;
(b) When required by system changes; and
(c) Within every three hundred sixty-five (365) days thereafter.</td></tr>
<tr><td colspan="2"><b>Discussion</b>
Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and organizational officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Managers responsible for contingency operations and technical personnel should meet, at a minimum, once a year for review of contingency policies and procedures. Each review session should be documented and confirm that appropriate training has been completed.</td></tr>
<tr><td colspan="2"><b>Implementation Standard</b></td></tr>
<tr><td><b>Control Review Frequency</b>
Quarterly</td><td><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td><b>Related Controls</b>
AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9;</td><td><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
FISCAM: AS-5, CP-2;
HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(D);
HSPD: HSPD 7 G(22)(i);
NIST SP: 800-16, 800-50;</td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="2"><b>HVA Discussion</b></td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>CP-03(01)</b></td><td><b>Control Name</b>
<b>Simulated Events</b></td><td><b>Priority</b></td><td><b>CMS Baseline</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
The use of simulated events creates an environment for personnel to experience actual threat events including cyber-attacks that disable web sites, ransom-ware attacks that encrypt organizational data on servers, hurricanes that damage or destroy organizational facilities, or hardware or software failures.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Quarterly</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
None;</td><td colspan="2"><b>Reference Policy</b>
HSPD: HSPD 7 G(22)(i);</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

Control Number **CP-03(2)**	**Control Name** **Mechanisms Used in Training Environments**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.			
Discussion Operational mechanisms refer to processes that have been established to accomplish an organizational goal or a system that supports a particular organizational mission or business objective. Actual mission and business processes, systems, and/or facilities may be used to generate simulated events and enhance the realism of simulated events during contingency training.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls		**Reference Policy** Federal Continuity Directive 1; NIST Special Publications 800-16, 800-50.	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CP-04**	**Control Name** **Contingency Plan Testing**	**Priority** **P3**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement (a) Test the contingency plan for the system at least every three hundred sixty-five (365) days using NIST (NIST SP 800-34 r1, NIST SP 800-84) and CMS -defined tests and exercises, such as tabletop tests, in accordance with the current CMS contingency plan procedure to determine the effectiveness of the plan and the readiness to execute the plan; (b) Review the contingency plan test results; and (c) Initiate corrective actions, if needed.			
Discussion Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2;
		Reference Policy
		FIPS: 199;
		NIST SP: 800-34, 800-84;	

Privacy Discussion Discussion for systems processing, storing, or transmitting PHI:			

Contingency plan tests and exercises should include an evaluation of the ability to meet privacy requirements in a contingency scenario as well as corrective measures to address any privacy risks identified.
Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the CMS Business/System.

Privacy Implementation Standards

HVA Control Statement

(a) Test the HVA contingency plan for the system at least every three hundred sixty-five (365) days using NIST (NIST SP 800-34, NIST SP 800-84) and CMS -defined tests and exercises, such as tabletop tests, in accordance with the current CMS contingency plan procedure to determine the effectiveness of the plan and the readiness to execute the plan;
(b) Review the HVA contingency plan test results; and
(c) Initiate corrective actions, if needed.

HVA Discussion

Methods for testing HVA contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations should conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
CP-04(01)	**Coordinate with Related Plans**		**Moderate** **High**

Control Statement

Coordinate contingency plan testing with organizational elements responsible for related plans.

Discussion

Plans related to contingency planning for organizational systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations coordinate with those elements.
Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission/business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope:

1. COOP
2. BCP
3. CIP Plan
4. DRP
5. ISCP
6. Cyber Incident Response Plan
7. OEP

Implementation Standard

High & Moderate:
Std.1 - Require a suite of plans to prepare for response, continuity, recovery, and resumption of mission/business processes and systems in the event of a disruption. Each plan has a specific purpose and scope:
(a) Continuity of Operations Plan (COOP)
(b) Business Continuity Plan (BCP)
(c) Critical Infrastructure Protection (CIP) Plan
(d) Disaster Recovery Plan (DRP)

(e) Information System Contingency Plan (ISCP) (f) Cyber Incident Response Plan (g) Occupant Emergency Plan (OEP)	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
IR-8, PM-8;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	HSPD: HSPD 7 G(22)(i);
	NIST SP: 800-34;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **CP-04(02)**	**Control Name** **Alternate Processing Site**	**Priority**	**CMS Baseline** **High**
Control Statement Test the contingency plan at the alternate processing site: (a) To familiarize contingency personnel with the facility and available resources; and (b) To evaluate the capabilities of the alternate processing site to support contingency operations.			
Discussion Conditions at the alternate processing site may be significantly different than the conditions at the primary site. Having the opportunity to visit the alternate site and experience, firsthand, the actual capabilities available at the site can provide valuable information on potential vulnerabilities that could affect essential organizational missions and functions. The on-site visit can also provide an opportunity to refine the contingency plan to address the vulnerabilities discovered during testing.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls CP-7;		**Reference Policy** HSPD: HSPD 7 G(22)(i);	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CP-04(04)**	**Control Name** **Full Recovery and Reconstitution**	**Priority** **P2**	**CMS Baseline** **Above Baseline**
Control Statement Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.			
Discussion Recovery is executing contingency plan activities to restore organizational missions and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Organizations establish a known state for systems that includes system state information for hardware, software programs, and data. Preserving system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission and business processes.			

Implementation Standard	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls CP-10, SC-24;	**Reference Policy** See CP-4;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CP-06	**Alternate Storage Site**	**P1**	**Moderate** **High**

Control Statement (a) Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and (b) Ensure that the alternate storage site provides controls equivalent to that of the primary site.
Discussion Alternate storage sites are sites that are geographically distinct from primary storage sites and that maintain duplicate copies of information and data if the primary storage site is not available. In contrast to alternate storage sites, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may also be considered as alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions and business functions despite disruption, compromise, or failure in organizational systems.
Implementation Standard

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;
	HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B);
	45 C.F.R. §164.310(a)(2)(i);
	NIST SP: 800-34

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CP-06(01)	**Separation from Primary Site**	**P1**	**Moderate** **High**
Control Statement			

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.	
Discussion Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls RA-3;	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CP-06(02)	**Recovery Time and Point Objectives**		**High**

Control Statement Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	
Discussion Organizations establish recovery time and recovery point objectives as part of contingency planning. Configuration of the alternate storage site includes physical facilities and the systems supporting recovery operations ensuring accessibility and correct execution.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls None;	**Reference Policy** See CP-6;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CP-06(03)	**Accessibility**		**Moderate** **High**

Control Statement Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.
Discussion Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls RA-3;	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CP-07	**Alternate Processing Site**		**Moderate** **High** **HVA**

Control Statement (a) Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of system operation types defined by CMS for essential missions and business functions within an allowable outage time consistent with recovery time and recovery point objectives (specified by the applicable system contingency plan or COOP for the business function(s) supported by the system) when the primary processing capabilities are unavailable; (b) Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time-period (specified in the applicable system contingency plan or COOP) for transfer and resumption; and (c) Provide controls at the alternate processing site that are equivalent to those at the primary site.	
Discussion Alternate processing sites are sites that are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives such as failover to a cloud-based service provider or other internally- or externally-provided processing service. Geographically distributed architectures that support contingency requirements may also be considered as alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites; access rules; physical and environmental protection requirements; and the coordination for the transfer and assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions and business functions despite disruption, compromise, or failure in organizational systems. Equipment and supplies required to resume operations within the CMS-defined period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with CMS recovery time objectives.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;
	HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B);
	45 C.F.R. §164.310(a)(2)(i);
	45 C.F.R. §164.308(7)(ii)(C);
	NIST SP: 800-34;
	PPD-21;

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): When an alternate processing site is used, administrative, physical and technical controls must be implemented to protect personally identifiable information (PII) in accordance with the privacy risks identified.	

Discussion for systems processing, storing, or transmitting PHI:
When an alternate processing site is used, administrative, physical and technical controls must be implemented to protect PHI in accordance with the CMS Business/System's risk analysis.

Privacy Implementation Standards

HVA Control Statement

(a) Establish a physical alternate processing site, including necessary agreements to permit the transfer and resumption of the HVA system operation types defined by CMS for essential missions and business functions within an allowable outage time consistent with recovery time and recovery point objectives (specified by the applicable system contingency plan or COOP for the business function(s) supported by the system) when the primary processing capabilities are unavailable;
(b) Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time-period (specified in the applicable system contingency plan or COOP) for transfer and resumption; and
(c) Provide controls at the alternate processing site that are equivalent to those at the primary site.

HVA Discussion

Alternate processing sites are sites that are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives such as failover to a cloud-based service provider or other internally- or externally-provided processing service. Geographically distributed architectures that support contingency requirements may also be considered as alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions and business functions despite disruption, compromise, or failure in organizational systems. This control may not be necessary for HVAs that are rated as 'Low' impact for availability.

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
CP-07(01)	**Separation from Primary Site**	**P1**	**Moderate** **High**

Control Statement

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats

Discussion

Threats that affect alternate processing sites are defined in organizational assessments of risk and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Implementation Standard

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls RA-3;	**Reference Policy** FedRAMP: Rev. 4 Baseline;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **CP-07(02)**	**Control Name** **Accessibility**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.			
Discussion Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls RA-3;		**Reference Policy** FedRAMP: Rev. 4 Baseline;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CP-07(03)**	**Control Name** **Priority of Service**	**Priority** **P1**	**CMS Baseline** **Moderate** **High** **HVA**
Control Statement Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).			
Discussion Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site. Organizations establish recovery time objectives as part of contingency planning.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls None;		**Reference Policy** FedRAMP: Rev. 4 Baseline;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Develop alternate processing site agreements that contain priority-of-service provisions in accordance with HVA availability requirements (including recovery time objectives). Establish recovery time objectives as part of contingency planning.			
HVA Discussion Priority-of-service agreements refer to negotiated agreements with service providers that provide organizations with priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site.			
HVA Implementation Standard			

Control Number **CP-07(04)**	**Control Name** **Preparation for Use**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Prepare the alternate processing site so that the site can serve as the operational site supporting essential missions and business functions.			
Discussion Site preparation includes establishing configuration settings for systems at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and logistical considerations are in place.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls CM-2, CM-6, CP-4;		**Reference Policy** See CP-7;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CP-08**	**Control Name** **Telecommunications Services**	**Priority** **P1**	**CMS Baseline** **Moderate** **High** **HVA**
Control Statement Establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for CMS essential missions and business functions within the resumption time specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.			
Discussion This control applies to telecommunications services (for data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions and business functions despite the loss of primary telecommunications services. Organizations may specify different time-periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines or the use of satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.			
Implementation Standard High: Std.1 - Ensure alternate telecommunications service level agreements (SLAs) are in place to permit resumption of system Recovery Time Objectives (RTO) and business functions Maximum Tolerable Downtimes (MTD) as specified in the applicable system contingency plan, BIA or COOP. Std.2 - Ensure alternate telecommunications service agreements are in place to permit resumption of system operations for essential missions and business functions within one (1) week of contingency plan activation when primary telecommunications capabilities are unavailable. Moderate: Std.1 - Ensure alternate telecommunications service level agreements (SLAs) are in place to permit resumption of system Recovery Time Objectives (RTO) and business functions Maximum Tolerable Downtimes (MTD) as specified in the applicable system contingency plan, BIA or COOP.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls		**Reference Policy**	

CP-2, CP-6, CP-7, CP-11, SC-7;	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-3;
	HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B);
	NIST SP: 800-34;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CP-08(01)	**Priority of Service Provisions**		**Moderate** **High**
Control Statement (a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and (b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.			
Discussion Organizations consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions. Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC) program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. The FCC sets the rules and policies for the TSP program and the Department of Homeland Security, manages the TSP program. The TSP program is always in effect and not contingent on a major disaster or attack taking place. Federal sponsorship is required to enroll in the TSP program			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls None;		**Reference Policy** FedRAMP: Rev. 4 Baseline;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CP-08(02)	**Single Points of Failure**	**P1**	**Moderate** **High**
Control Statement Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.			
Discussion In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is important to have provider transparency for the actual physical transmission capability for telecommunication services.			
Implementation Standard			
Control Review Frequency		**Assessment Frequency**	

Annually (365 Days)	Annually (365 Days)
Related Controls None;	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **CP-08(03)**	**Control Name** **Separation of Primary and Alternate Providers**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.			
Discussion Threats that affect telecommunications services are defined in organizational assessments of risk and include natural disasters, structural failures, cyber or physical attacks, and errors of omission or commission. Organizations can reduce common susceptibilities by minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls None;		**Reference Policy** See CP-8;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CP-08(04)**	**Control Name** **Provider Contingency Plan**	**Priority**	**CMS Baseline** **High**
Control Statement (a) Require primary and alternate telecommunications service providers to have contingency plans; (b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and (c) Obtain evidence of contingency testing and training by providers within every three hundred sixty-five (365) days.			
Discussion Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls		**Reference Policy**	

<table>
<tr><td>CP-3, CP-4;</td><td>See CP-8;</td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="2"><b>HVA Discussion</b></td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>CP-08(05)</b></td><td><b>Control Name</b>
<b>Alternate Telecommunications Service Testing</b></td><td><b>Priority</b></td><td><b>CMS Baseline</b>
<b>HVA</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Test alternate telecommunication services CMS-defined frequency].</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Alternate telecommunications services testing is arranged through contractual agreements with service providers. The testing may occur in parallel with normal operations to ensure that there is no degradation in organizational missions or functions.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
CP-3</td><td colspan="2"><b>Reference Policy</b>
NIST SP 800-34; National Communications Systems Directive 3-10;
Web: tsp.ncs.gov.</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b>
Test alternate telecommunication services at least every 6 months</td></tr>
<tr><td colspan="4"><b>HVA Discussion</b>
Alternate telecommunications services testing is arranged through contractual agreements with service providers. The testing may occur in parallel with normal operations to ensure there is no degradation in organizational missions or functions.</td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>CP-09</b></td><td><b>Control Name</b>
<b>System Backup</b></td><td><b>Priority</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b>
<b>HVA</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
(a) Conduct backups of user-level information contained in system components in accordance with the frequency specified in Implementation Standard 1;
(b) Conduct backups of system-level information contained in the system in accordance with the frequency specified in Implementation Standard 1;
(c) Conduct backups of system documentation, including security and privacy-related documentation and other forms of data, including paper records within the defined frequency (defined in the applicable security and privacy plan) consistent with recovery time and recovery point objectives; and
(d) Protect the confidentiality, integrity, and availability of backup information.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of backup information while in transit is outside the scope of this control. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Organizations may be subject to laws, executive orders, directives, regulations, or policies with requirements regarding specific</td></tr>
</table>

categories of information (e.g., personal health information). Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.
The transfer rate of backup information to an alternate storage site (if so designated) is guided by the CMS recovery time objectives and recovery point objectives. Checkpoint capabilities are part of any backup operation that updates files and consumes large amounts of information system time.

Implementation Standard

High & Moderate:
Std.1 - Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Three (3) generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups must be logged with name, date, time, and action.
Std.2 - Backups must be compliant with CMS requirements for protecting data at rest. (see SC-28)
Low:
Std.1 - Perform backups of user-level and system-level information (including system state information) every month.
Std.2 - Backups must be compliant with CMS requirements for protecting data at rest. (see SC-28)

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
CP-2, CP-6, CP-10, MP-4, MP-5, SI-4, SI-13, SC-13, SC-28;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;
	HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 45 C.F.R. §164.310(d)(2)(iv), 164.312(c)(1), 45 C.F.R. §164.308(a)(7)(ii)(C);
	NIST SP: 800-34;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
Backup copies of information need to be protected with the same level of security as if that information were being maintained on the original system. Applicable controls necessary to achieve this and to protect confidentiality include encryption of the backup. Backing up information helps maintain the integrity of the data—a requirement of the Privacy Act and HIPAA.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
High & Moderate:
PRIV.1 - Ensure that a current, retrievable, copy of personally identifiable information (PII) is available before movement of servers.
PRIV.2 - Use the encryption methodology specified in SC-13 to encrypt personally identifiable information (PII) confidentiality impact level information in backups at the storage location.
Systems processing, storing, or transmitting PHI:
High & Moderate:
PHI.1 - Establish procedures that create a retrievable, exact copy of the PHI before any movement of information system equipment.

HVA Control Statement

(a) Conduct backups of user-level information contained in system components in accordance with the frequency specified in Implementation Standard 1;
(b) Conduct backups of system-level information contained in the system in accordance with the frequency specified in Implementation Standard 1;
(c) Conduct backups of system documentation, including security and privacy-related documentation and other forms of data, including paper records within the defined frequency (defined in the applicable security and privacy plan) consistent with recovery time and recovery point objectives; and
(d) Protect the confidentiality, integrity, and availability of backup information.

HVA Discussion

System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of backup information while in transit is outside the scope of this control. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information.

Organizations may be subject to laws, executive orders, directives, regulations, or policies with requirements regarding specific categories of information (e.g., personal health information). Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

The transfer rate of backup information to an alternate storage site (if so designated) is guided by the CMS recovery time objectives and recovery point objectives. Checkpoint capabilities are part of any backup operation that updates files and consumes large amounts of information system time.

HVA Implementation Standard

High & Moderate:

Std.1 - Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Three (3) generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups must be logged with name, date, time, and action.

Std.2 - Backups must be compliant with CMS requirements for protecting data at rest. (see SC-28)

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CP-09(01)	**Testing for Reliability and Integrity**		**Moderate** **High** **HVA**

Control Statement

Test backup information at least every three months for High systems or six months for Moderate systems, to verify media reliability and information integrity.

Discussion

Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.

Implementation Standard

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Annually (365 Days)
Related Controls	**Reference Policy**
CP-4;	FedRAMP: Rev. 4 Baseline;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

Test backup information at least every three months for High systems or six months for Moderate systems, to verify media reliability and information integrity.

As part of the contingency planning processes, restore complete select HVA functions to ensure that backups are effective, personnel know how to perform function restores, and the function operates correctly once restored.

HVA Discussion

Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
CP-09(02)	**Test Restoration Using Sampling**	**P1**	**High**

Control Statement Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.	
Discussion Organizations need assurance that system functions can be restored correctly and can support established organizational missions. To ensure that the selected system functions are thoroughly exercised during contingency plan testing, a sample of backup information is used to determine if the functions operate as intended. Organizations can determine the sample size for the functions and backup information based on the level of assurance needed.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls CP-4;	**Reference Policy** See CP-9;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **CP-09(03)**	**Control Name** **Separate Storage for Critical Information**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Store backup copies of critical system software and other security-related information, as well as copies of the system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.			
Discussion Separate storage for critical information applies to all critical information regardless of the type of backup storage media. Critical system software includes operating systems, middleware, cryptographic key management systems, and intrusion detection systems. Security-related information includes inventories of system hardware, software, and firmware components. Alternate storage sites, including geographically distributed architectures, serve as separate storage facilities for organizations. Organizations may provide separate storage by implementing automated backup processes at alternative storage sites (e.g., data centers). The General Services Administration (GSA) establishes standards and specifications for security and fire-rated containers.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls CM-2, CM-6, CM-8;		**Reference Policy** FedRAMP: Rev. 4 Baseline;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **CP-09(05)**	**Control Name** **Transfer to Alternate Storage Site**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement			

Transfer system backup information to the alternate storage site at defined time periods (defined in the applicable security and privacy plan) and transfer rates (defined in the applicable security and privacy plan) consistent with the recovery time and recovery point objectives.	
Discussion System backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls CP-7, MP-3, MP-4, MP-5;	**Reference Policy** See CP-9;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **CP-09(08)**	**Control Name** **Cryptographic Protection**	**Priority**	**CMS Baseline** **Moderate** **High**

Control Statement Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of backup information.	
Discussion The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanisms selected is commensurate with the security category or classification of the information. This control enhancement applies to system backup information in storage at primary and alternate locations. Organizations implementing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
SC-12, SC-13, SC-28;
	Reference Policy
	FIPS: 140-3, FIPS 186-4;
	NIST SP: 800-34, 800-130, 800-152;

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): FIPS-validated cryptographic modules are the government standard for encryption. The implementation of cryptographic mechanisms to protect sensitive information (such as PII) at rest or in storage at primary and alternate locations must comply with these standards. CMS Businesses/Systems should use cryptographic mechanisms to prevent unauthorized disclosure and modification of system backup information containing PII.	
Privacy Implementation Standards Systems processing, storing, or transmitting PII (to include PHI): High & Moderate: PRIV.1 - Implement FIPS validated cryptographic mechanisms (FIPS 140-2, FIPS 140-3) to encrypt personally identifiable information (PII) confidentiality impact level information in backups at the storage location.	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **CP-10**	**Control Name** **System Recovery and Reconstitution**	**Priority**	**CMS Baseline** **Low** **Moderate** **High** **HVA**

Control Statement

Provide for the recovery and reconstitution of the system to a known state within defined time period (specified in the applicable security and privacy plan, contingency plan, or COOP) consistent with the recovery time and recovery point objectives after a disruption, compromise, or failure. Recovery of the system after a failure or other contingency must be done in a trusted, secure, and verifiable manner.

Discussion

Recovery is executing contingency plan activities to restore organizational missions and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point, recovery time, and reconstitution objectives, and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.

Implementation Standard

High, Moderate & Low:

Std.1 - Secure system recovery and reconstitution includes, but is not limited to:

(a) Reset all system parameters (either default or organization-established);

(b) Reinstall patches;

(c) Reestablish configuration settings;

(d) Reinstall application and system software; and

(e) Fully test the system.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
CA-2, CA-6, CA-7, CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;
	HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B);
	45 C.F.R. §164.308(a)(7)(ii)(C);
	HSPD: HSPD 7 G(22)(i);
	NIST SP: 800-34;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

System recovery and reconstitution is an important step to restoring sensitive information, such as both personally identifiable information (PII) and protected health information (PHI), to an accurate state following execution of a contingency plan.

Privacy Implementation Standards

HVA Control Statement

Provide for the recovery and reconstitution of the system to a known state within defined time period (specified in the applicable security and privacy plan, contingency plan, or COOP) consistent with the recovery time and recovery point objectives after a disruption, compromise, or failure. Recovery of the system after a failure or other contingency must be done in a trusted, secure, and verifiable manner.

HVA Discussion

<table>
<tr><td>Recovery is executing contingency plan activities to restore organizational missions and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point, recovery time, and reconstitution objectives, and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.</td></tr>
<tr><td><b>HVA Implementation Standard</b>
Std.1 - Secure system recovery and reconstitution includes, but is not limited to:
(a) Reset all system parameters (either default or organization-established);
(b) Reinstall patches;
(c) Reestablish configuration settings;
(d) Reinstall application and system software; and
(e) Fully test the system.</td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>CP-10(02)</b></td><td><b>Control Name</b>
<b>Transaction Recovery</b></td><td><b>Priority</b></td><td><b>CMS Baseline</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Implement transaction recovery for systems that are transaction-based.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
None;</td><td colspan="2"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
NIST SP: 800-34</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>CP-10(04)</b></td><td><b>Control Name</b>
<b>Restore within Time Period</b></td><td><b>Priority</b></td><td><b>CMS Baseline</b>
<b>High</b>
<b>HVA</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Provide the capability to restore system components within the target restoration time (specified in applicable system contingency plan or disaster recovery plan) from configuration-controlled and integrity-protected information representing a known, operational state for the components.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Restoration of system components includes reimaging which restores the components to known, operational states.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b></td><td colspan="2"><b>Assessment Frequency</b></td></tr>
</table>

Annually (365 Days)	Three (3) Years
Related Controls CM-2, CM-6;	**Reference Policy** NIST SP: 800-34
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Provide the capability to restore system components within the target restoration time (specified in applicable system contingency plan or disaster recovery plan) from configuration-controlled and integrity-protected information representing a known, operational state for the components.	
HVA Discussion Restoration of HVA components includes reimaging which restores the components to known, operational states.	
HVA Implementation Standard Systems designated as HVA: High & Moderate: HVA.1 – Replace Control with: Provide the capability to restore HVA system components within the target restoration time (specified in applicable system contingency plan) from configuration-controlled and integrity-protected information representing a known, operational state for the components.	

Identification and Authentication

Control Number	Control Name	Priority	CMS Baseline
IA-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel and roles:

1. CMS Enterprise-level identification and authentication policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

(c) Review and update the current identification and authentication:

1. Policy at least every three (3) years; and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and

2. Procedures at least every three (3)years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines

Discussion

This control addresses policy and procedures for the controls in the IA family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise level identification and authentication policy within this CMS IS2P2, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures.)

Implementation Standard

High, Moderate & Low:

Std. 1 - The CMS CIO and CISO will (a) Develop, document, and disseminate to applicable personnel and roles:

1. CMS Enterprise-level identification and authentication policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

(c) Review and update the current identification and authentication:

1. Policy at least every three (3) years; and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and

2. Procedures at least every three (3)years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

AC-1, PM-9, PS-8, SI-12;	FedRAMP: Rev. 4 Baseline;
	FIPS: 201-2;
	FISCAM: AC-2.1.1, AC-2.1.4, AC-4.1.1, AS-1, AS-2.2, AS-2.3.2, SM-1, SM-3;
	NISTIR: 7874;
	NIST SP: 800-12, 800-30, 800-39, 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-100;
	OMB Circular: A-130;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
Privacy considerations should be included in identification and authentication policy and procedures, especially when the system contains information subject to the Privacy Act and/or HIPAA.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
High & Moderate:
PRIV.1 - Monitor for changes to applicable privacy laws, regulations, and overarching policy that affect identification and authentication policies no less often than once every 365 days to ensure the CMS and Mission/Business/System identification and authentication policies remains effective.
PRIV.2 - Ensure identification and authentication policies support privacy to the greatest extent feasible throughout the system's life cycle.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
IA-02	**Identification and Authentication (Organizational Users)**	**P1**	**Low Moderate High HVA**

Control Statement

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Discussion

Organizations can satisfy the identification and authentication requirements by complying with the requirements in Homeland Security Presidential Directive (HSPD) 12 (Policy for a Common Identification Standard for Federal Employees and Contractors). Organizational users include employees or individuals that organizations consider having equivalent status of employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than accesses that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.

Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities, or in the case of multifactor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.

The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-8.

CMS Mission/Business/System implementations managing organizational users are required to follow the Identity, Credential, and Access Management (ICAM), sometimes also known as Identity and Access Management (IDAM), requirements as defined under OMB M-19-17 (Enabling Mission Delivery through Improved Identity, Credential, and Access Management) and under HHS Guidance for Selection of e-Authentication Assurance Levels. These policies require the implementation of NIST SP 800-63-3 (Digital Identity Guidelines). Implementation of the Federal PIV, or a NIST approved equivalent (i.e., by contractors), will fulfill this control.

<table>
<tr><td colspan="2">Organizational Users are defined by NIST (HYPERLINK "https://csrc.nist.gov/glossary/term/Organizational User") as an organizational employee or an individual the organization deems to have equivalent status of an employee including, for example, contractor, guest researcher, or individual detailed from another organization.</td></tr>
<tr><td colspan="2"><b>Implementation Standard</b>
High, Moderate & Low:
Std.1 - Employ effective identity proofing and authentication processes, compliant with HHS and NIST SP 800-63-3, for organizational users when CMS Sensitive information (e.g., CUI, PII, PHI) is to be accessed, modified, or released.
Std.2 - Require the use of system and/or network authenticators and unique user identifiers for organizational users.
Std.3 - Help desk support requires user identification for any transaction that has information security and privacy implications.</td></tr>
<tr><td><b>Control Review Frequency</b>
Six (6) Months</td><td><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td><b>Related Controls</b>
AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA-5, PE-2, PL-4, SA-4, SA-8;</td><td><b>Reference Policy</b>
Statute: FISMA 2014;
FedRAMP: Rev. 4 Baseline;
FIPS: 140-2/140-3, 201-2, 202;
FISCAM: AC-2, AC-2.1.1, AC-2.1.4, AC-4.1.1, AS-2, AS-2.2; AS-2.3.2;
HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D), 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(d);
NISTIR: 7539, 7676, 7817, 7849, 7870, 7874, 7966;
NIST SP: 800-63-3, 800-63A, 800-63B, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166;
OMB Memo: M-06-16, M-16-04, M-19-03, M-19-17;
Web: HYPERLINK "https://www.idmanagement.gov/" ;</td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b>
(a) HVA Systems must use multifactor authentication (MFA) to uniquely identify all organizational users and systems or services acting on behalf of organizational users.
(b) System and Service accounts must not utilize well known account IDs and used as intended and authorized.
.</td></tr>
<tr><td colspan="2"><b>HVA Discussion</b>
Each user is uniquely identified with multifactor authentication. Password only authenticators for users or privileged accounts and group/shared accounts are not allowed for access to the HVA. System and Service accounts should not utilize well known account identifications (IDs) (e.g., system administrator (SA), root, administrator, etc.). System and service accounts are only used as intended and authorized. HVA users are not permitted to logon to any system using the system or service accounts. User accounts are not to be used as a system or service account.</td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>IA-02(01)</b></td><td><b>Control Name</b>
<b>Multifactor Access to Privileged Accounts</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b>
<b>HVA</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Implement multifactor authentication for access to privileged accounts.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Multifactor authentication (MFA) requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number (PIN)); something you have (e.g., a physical authenticator or cryptographic private key stored in hardware or software); or something you are (e.g., a biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security.</td></tr>
</table>

Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multifactor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access. For privileged organizational users (any user with elevated levels of privileges), HHS and CMS require a minimum of two-factor authentication (e.g., personal identity verification (PIV) and personal identification number (PIN)) to gain access to the system. Implemented authentication mechanisms, to include two-factor authentication, used to authenticate privileged organizational users must comply with HHS and CMS Identification, Credential, and Access Management (ICAM) standards.	
Implementation Standard High, Moderate & Low: Std. 1 - Implement multifactor authentication for access to privileged accounts.	
Control Review Frequency Six (6) Months	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-5, AC-6;
	Reference Policy
	Statute: FISMA 2014;
	FedRAMP: Rev. 4 Baseline;
	FIPS: 140-2/140-3, 201;
	NIST SP: 800-63-3;
	OMB Circular: A-130;
	OMB Memo: M-16-04, M-19-03, M-19-17;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement (a)Privileged accounts each HVA using multifactor authentication mechanisms to protect against password weaknesses. (b) All HVA systems and devices must support and implement authentication of privileged accounts through multifactor authentication.	
HVA Discussion Multifactor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator or cryptographic private key stored in hardware or software), or something you are (e.g., a biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multifactor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.	
HVA Implementation Standard	

Control Number **IA-02(02)**	**Control Name** **Multifactor Access to Non-Privileged Accounts**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement Implement multifactor authentication for access to non-privileged accounts.			
Discussion Multifactor authentication (MFA) requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number (PIN)); something you have (e.g., a physical authenticator or cryptographic private key stored in hardware or software); or something you are (e.g., a biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the			

system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access, privileged accounts are authenticated using multifactor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

For non-privileged organizational users (the normal user), CMS requires a minimum of two-factor authentication (e.g., personal identity verification (PIV) and personal identification number (PIN)) to gain access to the system. Implemented authentication mechanisms, to include two-factor authentication, used to authenticate non-privileged organizational users must comply with HHS and CMS Identification, Credential, and Access Management (ICAM) standards.

Implementation Standard

High, Moderate & Low:

Std. 1 - Implement multifactor authentication for access to non-privileged accounts.

Control Review Frequency	**Assessment Frequency**
Six (6) Months	Annually (365 Days)

Related Controls	**Reference Policy**

AC-5;	Statute: FISMA 2014;
	FedRAMP: Rev. 4 Baseline;
	FIPS: 140-2/140-3, 201;
	NIST SP: 800-63-3;
	OMB Circular: A-130;
	OMB Memo: M-16-04, M-19-03, M-17-19;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA.1 – Replace Control with:

(a) Non-privileged accounts are authenticated on each system using multifactor authentication (MFA) mechanisms that protect against password weaknesses.

(b) All HVA systems and devices must support and implement authentication of non-privileged accounts through multifactor authentication.

HVA Discussion

All systems and devices support and implement authentication of non-privileged accounts through multifactor authentication.

Multifactor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a PIN), something you have (e.g., a physical authenticator or cryptographic private key stored in hardware or software), or something you are (e.g., a biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the DoD CAC. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access, privileged accounts are authenticated using multifactor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
IA-02(05)	**Individual Authentication with Group Authentication**	**P1**	**High**

Control Statement

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

Discussion

Individual authentication prior to shared group authentication helps to mitigate the risk of using group accounts or authenticators.

Implemented shared account authentication mechanisms must comply with HHS and CMS Identification, Credential, and Access Management (ICAM) standards.

Implementation Standard

High:

Std. 1 - When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

Control Review Frequency	**Assessment Frequency**

Annually (365 Days)	Three (3) Years
Related Controls None;	**Reference Policy** See Control IA-2;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **IA-02(06)**	**Control Name** **ACCESS TO ACCOUNTS — SEPARATE DEVICE**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Implement multi-factor authentication for network access to privileged accounts such that: (a) One of the factors is provided by a device separate from the system gaining access; and (b) The device meets minimum token requirement.			
Discussion			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls AC-6		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **IA-02(08)**	**Control Name** **Access to Accounts - Replay Resistant**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement Implement replay-resistant authentication mechanisms for access to privileged accounts and non-privileged accounts.			
Discussion Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators.			
Implementation Standard High, Moderate & Low: Std. 1 - Implement replay-resistant authentication mechanisms for access to privileged accounts and non-privileged accounts.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
None;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		OMB Memo: M-16-04, M-19-03;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			

HVA Discussion
HVA Implementation Standard

Control Number **IA-02(12)**	**Control Name** **Acceptance of PIV Credentials**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement Accept and electronically verify Personal Identity Verification-compliant credentials.			
Discussion Acceptance of Personal Identity Verification (PIV)-compliant credentials applies to organizations implementing logical access control and physical access control systems. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. The adequacy and reliability of PIV card issuers are authorized using NIST SP 800-79-2. Acceptance of PIV-compliant credentials includes derived PIV credentials, the use of which is addressed in NIST SP 800-166. The DOD Common Access Card (CAC) is another example of a compliant credential.			
Implementation Standard High, Moderate & Low: Std. 1 - Accept and electronically verify Personal Identity Verification-compliant credentials.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	

Related Controls
AU-2, PE-3, SA-4;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		FIPS: 201;
		HSPD: HSPD 12;
		NIST SP: 800-63-3, 800-79-2, 800-166;
		OMB Circular: A-130;
		OMB Memo: M-16-04, M-19-03;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement (a) Identification and authentication to HVA must be facilitated using PIV in compliance with FIPS Publication 201-1 and OMB M-11-11. (b) Additional authentication factors must be employed in a risk-based manner.			
HVA Discussion Acceptance of PIV-compliant credentials applies to organizations implementing logical access control and physical access control systems. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. The adequacy and reliability of PIV card issuers are authorized using (NIST SP 800-79-2). Acceptance of PIV-compliant credentials includes derived PIV credentials, the use of which is addressed in (NIST SP 800-166). The DOD CAC is an example of a PIV credential.			
HVA Implementation Standard			

Control Number **IA-03**	**Control Name** **Device Identification and Authentication**	**Priority** **P2**	**CMS Baseline** **Moderate** **High** **HVA**
Control Statement Uniquely identify and authenticate devices (defined in applicable security/privacy plans) that require authentication mechanisms, which, at a minimum, use shared information (MAC or IP address) and access control lists to control remote network access before establishing a remote connection. If remote authentication is provided by the system itself,			

<table>
<tr><td colspan="2">the system must be in compliance with OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies (HYPERLINK "https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2004/m04-04.pdf").</td></tr>
<tr><td colspan="2"><b>Discussion</b>
Devices that require unique device-to-device identification and authentication are defined by type, by device, or by a combination of type and device. Organization-defined device types can include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Because of the challenges of implementing device authentication on large scale, organizations can restrict the application of the control to a limited number (and type) of devices based on need.
At a minimum, CMS systems should be filtered by MAC and/or IP address when accessing remote systems. OMB Memo M-04-04, in conjunction with NIST SP 800-63-3, provides remote authentication guidance (and minimal requirements) for remote authentication when remote access provided by the system.</td></tr>
<tr><td colspan="2"><b>Implementation Standard</b>
High, Moderate & Low:
Std. 1 - Uniquely identify and authenticate devices (defined in applicable security/privacy plans) that require authentication mechanisms, which, at a minimum, use shared information (MAC or IP address) and access control lists to control remote network access before establishing a remote connection. If remote authentication is provided by the system itself, the system must be in compliance with OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies (HYPERLINK "https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2004/m04-04.pdf").</td></tr>
<tr><td><b>Control Review Frequency</b>
Annually (365 Days)</td><td><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td><b>Related Controls</b>
AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4;</td><td><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
FISCAM: AC-2, AC-2.1.1, AC-2.1.4, AC-2.1.5, AC-2.1.6, AC- 2.1.8, AC-4.1.1, AS-2, AS-2.2, AS-2.3.2;
HIPAA: 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(d), 45 C.F.R. §164.312(a)(1);
OMB Circular: A-130;
OMB Memo: M-19-17;</td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b>
(a) Devices must be authenticated to protect against unauthorized access to HVA information and services by unauthorized devices.
(b) Validates security posture, uniquely identifies, and authenticates devices before establishing a network connection to the HVA.</td></tr>
<tr><td colspan="2"><b>HVA Discussion</b>
Devices that require unique device-to-device identification and authentication are defined by type, by device, or by a combination of type and device. Organization-defined device types can include devices that are not owned by the organization. Systems use shared known information (e.g., MAC and Transmission Control Protocol (TCP)/IP addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers) 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-TLS authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations should determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Because of the challenges of implementing device authentication on large scale, organizations can restrict the application of the control to a limited number (and type) of devices based on need</td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>IA-04</b></td><td><b>Control Name</b>
<b>Identifier Management</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Manage system identifiers by:
(a) Receiving authorization from defined personnel or roles (defined in applicable security/privacy plans) to assign an individual, group, role, service, or device identifier;</td></tr>
</table>

(b) Selecting an identifier that identifies an individual, group, role, service, or device;
(c) Assigning the identifier to the intended individual, group, role, service, or device; and
(d) Preventing reuse of identifiers for three (3) years.

Note: Prevention of identifier reuse includes ensuring previous identifier-based access authorizations are removed from the system. For example, if an identifier has provided access to one or more sensitive files or folders, before the identifier can be reused, the identifier-based access must be removed from the files and folders.

Discussion

Common device identifiers include media access control (MAC), Internet Protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names of the system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

Implementation Standard

High, Moderate & Low:

Std. 1 - Manage system identifiers by:
(a) Receiving authorization from defined personnel or roles (defined in applicable security/privacy plans) to assign an individual, group, role, service, or device identifier;
(b) Selecting an identifier that identifies an individual, group, role, service, or device;
(c) Assigning the identifier to the intended individual, group, role, service, or device; and
(d) Preventing reuse of identifiers for three (3) years.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years

Related Controls	**Reference Policy**

AC-2, IA-2, IA-3, IA-5, IA-8, IA-9, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS-3, PS-4, PS-5, SC-37;	FedRAMP: Rev. 4 Baseline;
	FIPS: 201-2;
	FISCAM: AC-2, AC-2.1.12, AC-2.1.16, AS-2;
	HIPAA: 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(d), 45 C.F.R. §164.308(a)(4), 45 C.F.R. §164.308(a)(5)(ii)(D);
	NIST SP: 800-63-3, 800-73-4, 800-76-2, 800-78-4;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
IA-04(04)	**Identify User Status**	**P1**	**Moderate** **High**

Control Statement

Manage individual identifiers by uniquely identifying each individual using one or more CMS-defined characteristics identifying individual status (defined in applicable security/privacy plans).

Discussion

Characteristics identifying the status of individuals include contractors and foreign nationals. Identifying the status of individuals by characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.

Implementation Standard

High & Moderate:

Std. 1 - Manage individual identifiers by uniquely identifying each individual using one or more CMS-defined characteristics identifying individual status (defined in applicable security/privacy plans).	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls None;	**Reference Policy** See Control IA-4;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
IA-05	**Authenticator Management**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

Manage system authenticators by:

(a) Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

(b) Establishing initial authenticator content for any authenticators issued by the organization;

(c) Ensuring that authenticators have sufficient strength of mechanism for their intended use;

(d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

(e) Changing default authenticators prior to first use;

(f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

(g) Protecting authenticator content from unauthorized disclosure and modification;

(h) Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

(i) Changing authenticators for group or role accounts when membership to those accounts changes.

(j) Changing or refreshing authenticators as follows:

−

− Passwords are no longer valid in the event of known or suspected compromise, and require immediate change;

− Passwords must be changed immediately upon system installation (e.g. default or vendor-supplied passwords);

− PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three (3) years; and

− Any PKI authentication request must be validated by Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) to ensure that the certificate being used for authentication has not been revoked.

(k) Changing, refreshing, or revoking PIV authenticators as follows:

− PIV compliant access cards are valid for no longer than five (5) years;

− The minimum PIN length for PIV cards shall be at least 6 digits;

− The maximum allowed PIN attempts for each PIV card stock is specified below:

• Fifteen (15) attempts – for 64k card stock in either Cybertrust / Verizon Business CA or those converted to Entrust certificates (64k card stock only); and

• Ten (10) attempts – for modern 128k cards issued by the Entrust CA.

Discussion

Authenticators include passwords, cryptographic devices, one-time password devices, and key cards. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements about authenticator content contain specific characteristics or criteria (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges. Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators; not sharing authenticators with others; and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

The 2018 modification to the HHS IS2P specifies the requirements for the maximum login attempts allowed when using ID and Password to authenticate to information systems; however, it does not include the maximum login attempts when authenticating with a PIV card. The maximum Personal Identification Number (PIN) attempts allowed for PIV cards is specified by policies implemented within the Smart Card Management System (SCMS) during issuance. These policies vary depending on a combination of card stock (64k, 128k), and certificate issuer for HHS (Cybertrust/Verizon Business CA or Entrust) and type of credential (PIV, RLA, ALT).

The maximum allowed PIN attempts for each PIV card stock is specified below:

• Fifteen (15) attempts – for 64k card stock in either Cybertrust / Verizon Business CA or those converted to Entrust certificates (64k card stock only); and
• Ten (10) attempts – for modern 128k cards issued by the Entrust CA.

Implementation Standard

High, Moderate & Low:

Std. 1 - Manage system authenticators by:

(a) Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
(b) Establishing initial authenticator content for any authenticators issued by the organization;
(c) Ensuring that authenticators have sufficient strength of mechanism for their intended use;
(d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
(e) Changing default authenticators prior to first use;
(f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
(g) Protecting authenticator content from unauthorized disclosure and modification;
(h) Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
(i) Changing authenticators for group or role accounts when membership to those accounts changes.
(j) Changing or refreshing authenticators as follows:
− Passwords are no longer valid in the event of known or suspected compromise, and require immediate change;
− Passwords must be changed immediately upon system installation (e.g. default or vendor-supplied passwords);
− PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three (3) years; and
− Any PKI authentication request must be validated by Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) to ensure that the certificate being used for authentication has not been revoked.
(k) Changing, refreshing, or revoking PIV authenticators as follows:
− PIV compliant access cards are valid for no longer than five (5) years;
− The minimum PIN length for PIV cards shall be at least 6 digits;
− The maximum allowed PIN attempts for each PIV card stock is specified below:
• Fifteen (15) attempts – for 64k card stock in either Cybertrust / Verizon Business CA or those converted to Entrust certificates (64k card stock only); and
• Ten (10) attempts – for modern 128k cards issued by the Entrust CA.

Control Review Frequency Two (2) Months	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FIPS: 140-2/140-3, 180-4, 201-2, 202;
	FISCAM: AC-2, AS-2;
	HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D), 45 C.F.R. §164.308(a)(3), 45 C.F.R. §164.308(a)(5)(ii)(D), 45 C.F.R. §164.312(d);
	NISTIR: 7539, 7817, 7849, 7870, 8040;

	NIST SP: 800-63-3, 800-73-4, 800-76-2, 800-78-4;
	OMB Circular: A-130;
	OMB Memo: M-16-04, M-19-03, M-19-17;
	Web: HYPERLINK "https://www.idmanagement.gov/" ;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
Adequate security to ensure confidentiality for any system containing sensitive information such as personally identifiable information (PII) is achieved through the management of the authenticators permitting access to that system. Authenticator management includes periodically changing passwords or other identifiers (e.g., certification and signatures) to reinforce identity validation and adherence to administrative security policies as well as enforces a time-based restriction on access, all of which bound access to PII in some way, limiting exposure in the event a user account is compromised.
Discussion for systems processing, storing, or transmitting PHI:
Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the CMS Business/System.

Privacy Implementation Standards

HVA Control Statement

Manage system authenticators by:
(a) Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
(b) Establishing initial authenticator content for any authenticators issued by the organization;
(c) Ensuring that authenticators have sufficient strength of mechanism for their intended use;
(d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
(e) Changing default authenticators prior to first use;
(f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
(g) Protecting authenticator content from unauthorized disclosure and modification;
(h) Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
(i) Changing/refreshing authenticators at least annually for cryptographic devices.
(j) Changing or refreshing authenticators as follows:
− Passwords are valid for no longer than sixty (60) days before they must be changed;
− Passwords are no longer valid in the event of known or suspected compromise, and require immediate change;
− Passwords must be changed immediately upon system installation (e.g. default or vendor-supplied passwords);
− PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three (3) years; and
− Any PKI authentication request must be validated by Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) to ensure that the certificate being used for authentication has not been revoked.
-Changing/refreshing authenticators at least annually or upon departure of key personnel with knowledge of password for service and system account passwords/pins
(k) Changing, refreshing, or revoking PIV authenticators as follows:
− PIV compliant access cards are valid for no longer than five (5) years;
− The minimum PIN length for PIV cards shall be at least 6 digits;
− The maximum allowed PIN attempts for each PIV card stock is specified below:
• Fifteen (15) attempts – for 64k card stock in either Cybertrust / Verizon Business CA or those converted to Entrust certificates (64k card stock only); and
• Ten (10) attempts – for modern 128k cards issued by the Entrust CA

HVA Discussion

Authenticators include passwords, cryptographic devices, one-time password devices, and key cards. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements about authenticator content contain specific characteristics or criteria (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual

<table>
<tr><td>authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges. Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum-length passwords, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.</td></tr>
<tr><td><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>IA-05(01)</b></td><td><b>Control Name</b>
<b>Password-Based Authentication</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b>
<b>HVA</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
For password-based authentication, systems follow the direction within the applicable baseline configuration (defined under CM-6) or, if more stringent, the following:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list using a frequency defined in applicable security/privacy plans, not to exceed three-hundred sixty-five (365) days, and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on CMS and Mission/Business/System-defined lists of commonly-used, expected, compromised passwords, or within a dictionary (names, words);
(c) Transmit only cryptographically-protected passwords following SI-07(06);
(d) Store passwords using an approved hash algorithm and salt, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery (i.e., use of temporary passwords will trigger an immediate change to a permanent password);
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules:
− MinimumPasswordLength = Minimum length of eight (8) characters for regular user passwords, and minimum length of fifteen (15) characters for administrator or privileged user passwords;
− PasswordComplexity = minimum (three (3) for High or one (1) for Moderate or Low) character(s) from the four (4) character categories (A-Z, a-z, 0-9, Special Characters);
− PasswordHistorySize = twelve (12) passwords for High or six (6) passwords for Moderate and Low systems; and
− If supported, enforce a minimum of number of changed characters:
MinimumCharactersChanged = at least 75% of characters
Note: This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., PIV cards). Also, administrator/privileged users are defined as those authorized for limited administrative purposes only based on business or technical need. Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.
Mobile devices are excluded from the password complexity requirement.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Password-based authentication applies to passwords regardless of whether they are used in single-factor or multifactor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefit while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically-protected passwords following SI-07(06) include salted one-way cryptographic hashes of passwords. The list of commonly-used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context specific words, for example, the name of the service, username, and derivatives thereof.</td></tr>
</table>

At CMS, passwords can be used as one of the factors (something the user knows) within a multifactor authentication mechanism. Additionally, password attributes (e.g., length, composition, histories) vary based on the role assigned to the user of the account (e.g., elevated privileged user vs. normal user) and the system's security impact level.
CMS is discouraging starting or ending passwords with a number. Systems and applications still exist where such passwords (beginning or ending with a number) are known to cause problems.
Mobile devices are excluded from the password complexity requirement.

Implementation Standard

High, Moderate & Low:
Std. 1 - For password-based authentication, systems follow the direction within the applicable baseline configuration (defined under CM-6) or, if more stringent, the following:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list using a frequency defined in applicable security/privacy plans, not to exceed three-hundred sixty-five (365) days, and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on CMS and Mission/Business/System-defined lists of commonly-used, expected, compromised passwords, or within a dictionary (names, words);
(c) Transmit only cryptographically-protected passwords following SI-07(06);
(d) Store passwords using an approved hash algorithm and salt, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery (i.e., use of temporary passwords will trigger an immediate change to a permanent password);
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules:

- MinimumPasswordLength = Minimum length of eight (8) characters for regular user passwords, and minimum length of fifteen (15) characters for administrator or privileged user passwords;
- PasswordComplexity = minimum (three (3) for High or one (1) for Moderate or Low) character(s) from the four (4) character categories (A-Z, a-z, 0-9, Special Characters);
- PasswordHistorySize = twelve (12) passwords for High or six (6) passwords for Moderate and Low systems; and
- If supported, enforce a minimum of number of changed characters:
  MinimumCharactersChanged = at least 75% of characters

Note: This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., PIV cards). Also, administrator/privileged users are defined as those authorized for limited administrative purposes only based on business or technical need. Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.
Mobile devices are excluded from the password complexity requirement.

Control Review Frequency Two (2) Months	**Assessment Frequency** Annually (365 Days)

Related Controls
IA-6;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FIPS: 201-2;
	FISCAM: AC-2, AS-2;
	HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D), 45 C.F.R. §164.308(a)(3), 45 C.F.R. §164.308(a)(5)(ii)(D), 45 C.F.R. §164.312(d);
	NIST SP: 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-132;
	OMB Circular: A-130;
	OMB Memo: M-16-04, M-19-03, M-19-17;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA.1 – Replace Control with:

User and privileged accounts must comply with multifactor authentication requirements. Service and System accounts that leverage password based authentication shall meet the following requirements:

(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list using a frequency defined in applicable security/privacy plans, not to exceed three-hundred sixty-five (365) days, and when organizational passwords are suspected to have been compromised directly or indirectly;

(b) Verify, when users create or update passwords, that the passwords are not found on CMS and Mission/Business/System-defined lists of commonly-used, expected, compromised passwords, or within a dictionary (names, words);

(c) Transmit only cryptographically-protected passwords;

(d) Store passwords using an approved hash algorithm and salt, preferably using a keyed hash;

(e) Require immediate selection of a new password upon account recovery (i.e., use of temporary passwords will trigger an immediate change to a permanent password);

(f) Allow user selection of long passwords and passphrases using letters;

(g) Employ automated tools to assist the user in selecting strong password authenticators;

(h) Enforce the following composition and complexity rules:

- MinimumPasswordAge = one (1) day;
- MaximumPasswordAge = sixty (60) days;
- MinimumPasswordLength = Minimum length of twenty (20) characters;
- PasswordComplexity = minimum (3) character(s) from each of the two (2) character categories (A-Z, a-z) - no numbers or special characters;
- PasswordHistorySize = reuse is disallowed; and
- If supported, enforce a minimum of number of changed characters:
  MinimumCharactersChanged = at least 75% of characters
- Must NOT contain the username:
  Embedded Username = false

(i) Use of default authentication credentials is disallowed;

(j) As applicable, change upon personnel turnover;

(k) When applicable, passwords must be stored in a secured location and only used when necessary; and

(l) Passwords must be unique for each identifier and on each system within the HVA boundary.

HVA Discussion

Password-based authentication applies to passwords regardless of whether they are used in single-factor or multifactor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefit while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically-protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly-used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context specific words, for example, the name of the service, username, and derivatives thereof.

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
IA-05(02)	**Public Key-Based Authentication**	**P2**	**Moderate** **High**

Control Statement

(a) For public key-based authentication:

1. Enforce authorized access to the corresponding private key; and
2. Map the authenticated identity to the account of the individual or group; and

(b) When public key infrastructure (PKI) is used:

1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
2. Implement a local cache of revocation data to support path discovery and validation.

Discussion

Public key cryptography is a valid authentication mechanism for individuals and machines or devices. When PKI is implemented, status information for certification paths includes certificate revocation lists or certificate status protocol responses. For PIV cards, certificate validation involves the construction and verification of a certification path to the Common Policy Root trust anchor which includes certificate policy processing. Implementing a local cache of revocation data to support path discovery and validation supports system availability in situations where organizations are unable to access revocation information via the network.

Implementation Standard

High & Moderate

Std. 1 - (a) For public key-based authentication:

1. Enforce authorized access to the corresponding private key; and
2. Map the authenticated identity to the account of the individual or group; and

(b) When public key infrastructure (PKI) is used:

1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
2. Implement a local cache of revocation data to support path discovery and validation.

Control Review Frequency	**Assessment Frequency**
Quarterly	Annually (365 Days)
Related Controls	**Reference Policy**
IA-3, IA-6, SC-17;	FedRAMP: Rev. 4 Baseline;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
IA-05(06)	**Protection of Authenticators**	**P2**	**Moderate** **High**

Control Statement

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Discussion

For systems containing multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems. Security categories of information are determined as part of the security categorization process.

Implementation Standard

High & Moderate

Std. 1 - Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**
RA-2;	See Control IA-5;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number IA-05(15)	**Control Name** **GSA-APPROVED PRODUCTS AND SERVICES**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Use only General Services Administration-approved products and services for identity, credential, and access management.			
Discussion			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **IA-06**	**Control Name** **Authenticator Feedback**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.			
Discussion Authenticator feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, for example, desktops or notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems, for example, mobile devices with small displays, the threat may be less significant, and is balanced against the increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authenticator feedback is selected accordingly. Obscuring authenticator feedback includes displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before obscuring it.			
Implementation Standard High, Moderate & Low: Std. 1 - Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
AC-3, PE-18;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		FISCAM: AC-2, AC-2.1.17, AS-2;
		HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D), 45 C.F.R. §164.312(a)(1);	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

<table>
<tr><td>Control Number
IA-07</td><td>Control Name
Cryptographic Module Authentication</td><td>Priority
P1</td><td>CMS Baseline
Low
Moderate
High</td></tr>
<tr><td colspan="4">Control Statement
Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.</td></tr>
<tr><td colspan="4">Discussion
Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.</td></tr>
<tr><td colspan="4">Implementation Standard
High, Moderate & Low:
Std. 1 - Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.</td></tr>
<tr><td colspan="2">Control Review Frequency
Annually (365 Days)</td><td colspan="2">Assessment Frequency
Annually (365 Days)</td></tr>
<tr><td colspan="2">Related Controls
AC-3, IA-5, SA-4, SC-12, SC-13;</td><td colspan="2">Reference Policy
FedRAMP: Rev. 4 Baseline;
FIPS: 140-2/140-3;
FISCAM: AC-4, AS-2;
HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D), 45 C.F.R.§164.312(a)(2)(iv);
Web: HYPERLINK "https://csrc.nist.gov/projects/cryptographic-module-validation-program" ;</td></tr>
<tr><td colspan="4">Privacy Discussion</td></tr>
<tr><td colspan="4">Privacy Implementation Standards</td></tr>
<tr><td colspan="4">HVA Control Statement</td></tr>
<tr><td colspan="4">HVA Discussion</td></tr>
<tr><td colspan="4">HVA Implementation Standard</td></tr>
</table>

<table>
<tr><td>Control Number
IA-08</td><td>Control Name
Identification and Authentication (Non-Organizational Users)</td><td>Priority
P1</td><td>CMS Baseline
Low
Moderate
High</td></tr>
<tr><td colspan="4">Control Statement
Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users prior to gaining access to all Department systems and networks (unless a risk-based decision is made for a particular system that does not require non-organization user authentication).</td></tr>
<tr><td colspan="4">Discussion
Non-organizational users include system users other than organizational users explicitly covered by IA-2. Non-organizational users are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. Identification and authentication of non-organizational users accessing federal systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations consider many factors, including security, privacy, scalability, and practicality in balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.
CMS Mission/Business/System implementations managing non-organizational users are required to follow the Identity, Credential, and Access Management (ICAM), sometimes also known as Identity and Access Management (IDAM), requirements as defined under OMB M-19-17 (Enabling Mission Delivery through Improved Identity, Credential, and Access Management) and under HHS Guidance for Selection of e-Authentication Assurance Levels. These policies require the implementation of NIST SP 800-63-3 (Digital Identity Guidelines).</td></tr>
</table>

Non-Organizational Users are defined by NIST (HYPERLINK "https://csrc.nist.gov/glossary/term/non_organizational_user") as any user who is not an organizational user (which includes public users).	
Implementation Standard High, Moderate & Low: Std.1 - Employ effective identity proofing and authentication processes, compliant with HHS and NIST SP 800-63-3, for non-organizational users when CMS Sensitive information (e.g., CUI, PII, PHI) is to be accessed, modified, or released. Std.2 - Require the use of system and/or network authenticators and unique user identifiers for non-organizational users. Std.3 - Help desk support requires user identification for any transaction that has information security and privacy implications.	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA-3, SA-4, SA-12, SC-8;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FIPS: 201-2;
	HIPAA: 45 C.F.R. §164.312(a)(2)(i);
	NISTIR: 8062;
	NIST SP: 800-63-3, 800-63A, 800-63B, 800-79-2, 800-116;
	OMB Circular: A-130;
	OMB Memo: M-19-17;
	Web: HYPERLINK "https://www.idmanagement.gov/" ;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
IA-08(01)	**Acceptance of PIV Credentials from Other Agencies**	**P1**	**Low** **Moderate** **High**

Control Statement Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.	
Discussion Acceptance of Personal Identity Verification (PIV) credentials from other federal agencies applies to both logical and physical access control systems. PIV credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidelines. The adequacy and reliability of PIV card issuers are addressed and authorized using NIST SP 800-79-2.	
Implementation Standard High, Moderate & Low: Std. 1 - Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AU-2, PE-3, SA-4;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FIPS: 201-2;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	

<table>
<tr><td><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>IA-08(02)</b></td><td><b>Control Name</b>
<b>ACCEPTANCE OF EXTERNAL AUTHENTICATORS</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
(a) Accept only external authenticators that are NIST-compliant; and
(b) Document and maintain a list of accepted external authenticators.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Acceptance of only NIST-compliant external credentials applies to organizational systems that are accessible to the public (e.g., public-facing websites). External credentials are those credentials issued by nonfederal government entities. External credentials are certified as compliant with NIST SP 800-63-3 by an approved accreditation authority. Approved external credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. Meeting or exceeding federal requirements allows federal government relying parties to trust external credentials at their approved assurance levels.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High, Moderate & Low:
Std. 1 - (a) Accept only external authenticators that are NIST-compliant; and
(b) Document and maintain a list of accepted external authenticators.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Six (6) Months</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
AU-2;</td><td colspan="2"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
FIPS: 201-2;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>IA-08(04)</b></td><td><b>Control Name</b>
<b>Use of Defined Profiles</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Conform to NIST-issued profiles for identity management.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Conformance with NIST-issued profiles for identity management addresses open identity management standards. To ensure that open identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the United States Government assesses and scopes the standards and technology implementations against applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. The result is NIST-issued implementation profiles of approved protocols.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High, Moderate & Low:
Std. 1 - Conform to NIST-issued profiles for identity management.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
SA-4;</td><td colspan="2"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
FIPS: 201-2;</td></tr>
</table>

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **IA-11**	**Control Name** **Re-Authentication**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement Require users to re-authenticate when CMS-defined circumstances or situations occur requiring re-authentication as defined in applicable security/privacy plans.
Discussion In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when authenticators or roles change; when security categories of systems change; when the execution of privileged functions occurs; after a fixed time-period; or periodically.
Implementation Standard High, Moderate & Low: Std. 1 - Require users to re-authenticate when CMS-defined circumstances or situations occur requiring re-authentication as defined in applicable security/privacy plans. (a) Examples of CMS-defined or situations are; when authenticators or roles change, when security categories of systems change, when the execution of privileged functions occurs, or after a fixed time-period [CMS ODP TBD] at a minimum.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AC-3, AC-11, IA-2, IA-3, IA-8;
	Reference Policy
	HHS: HHS Guidance for Selection of e-Authentication Assurance Levels;
	NIST SP: 800-63-3;
	OMB Memo: M-19-17;

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **IA-12**	**Control Name** **Identity Proofing**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement (a) Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; (b) Resolve user identities to a unique individual; and (c) Collect, validate, and verify identity evidence.
Discussion Identity proofing is the process of collecting, validating, and verifying user's identity information for the purposes of issuing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts. Standards and guidelines specifying identity assurance levels for identity proofing include NIST SP 800-63-3 (Digital Identity Guidelines) and NIST SP 800-63A (Enrollment and Identity Proofing). At CMS, identity proofing establishes that a user (both organization or non-organizational) is who the user claims to be.
Implementation Standard

High & Moderate Std. 1 - (a) Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; (b) Resolve user identities to a unique individual; and (c) Collect, validate, and verify identity evidence.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8;
	Reference Policy
	HHS: HHS Guidance for Selection of e-Authentication Assurance Levels;
	NIST SP: 800-63-3, 800-63A, 800-79-2;
	OMB Memo: M-19-17;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **IA-12(02)**	**Control Name** **Identity Evidence**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**
Control Statement Require evidence of individual identification be presented to the registration authority.			
Discussion Identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries. The forms of acceptable evidence are consistent with the risk to the systems, roles, and privileges associated with the user's account.			
Implementation Standard High & Moderate Std. 1 - Require evidence of individual identification be presented to the registration authority.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	

Related Controls
None;
		Reference Policy
		HHS: HHS Guidance for Selection of e-Authentication Assurance Levels;
		NIST SP: 800-63-3, 800-63A, 800-79-2;
		OMB Memo: M-19-17;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **IA-12(03)**	**Control Name** **Identity Evidence Validation and Verification**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**
Control Statement			

Require that the presented identity evidence be validated and verified through CMS approved methods of validation and verification.	
Discussion Validating and verifying identity evidence increases the assurance that accounts, identifiers, and authenticators are being issued to the correct user. Validation refers to the process of confirming that the evidence is genuine and authentic, and the data contained in the evidence is correct, current, and related to an actual person or individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risk to the systems, roles, and privileges associated with the users account	
Implementation Standard High & Moderate Std. 1 - Require that the presented identity evidence be validated and verified through CMS approved methods of validation and verification.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
None;
	Reference Policy
	HHS: HHS Guidance for Selection of e-Authentication Assurance Levels;
	NIST SP: 800-63-3, 800-63A, 800-79-2;
	OMB Memo: M-19-17;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **IA-12(06)**	**Control Name** **ACCEPT EXTERNALLY-PROOFED IDENTITIES**	**Priority** **P2**	**CMS Baseline** **Above Baseline**
Control Statement Accept externally-proofed identities at CMS-defined identity assurance level.			
Discussion			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	

Related Controls
A-3, IA-4, IA-5, IA-8.
		Reference Policy
		HHS: HHS Guidance for Selection of e-Authentication Assurance Levels;
		NIST SP: 800-63-3, 800-63A, 800-79-2;
		OMB Memo: M-19-17;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Incident Response

Control Number	Control Name	Priority	CMS Baseline
IR-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel:

1. CMS Enterprise-level incident response policy that:
   (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the incident response policy and procedures; and

(c) Review and update the current incident response:

1. Policy within every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures within every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines)

Discussion

Incident response policy and procedures address the controls in the IR family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of incident response policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to incident response policy and procedures include assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise level incidence response policy within the CMS IS2P2, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures.)

Implementation Standard

High, Moderate & Low:

Std. 1 - The CIO and CISO will: (a) Develop, document, and disseminate to applicable personnel:

1. CMS Enterprise-level incident response policy that:
   (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the incident response policy and procedures; and

(c) Review and update the current incident response:

1. Policy within every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures within every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines)

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
PM-9, PS-8, SI-12.
(Redacted Privacy Controls: SE-2)
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-5, AS-1, AS-2, SM-1, SM-3;
	HIPAA: 45 C.F.R.§164.308(a)(6)(i), 45 C.F.R. §164.530(b)(1);
	NIST SP: 800-12, 800-61, 800-83, 800-100;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
In developing incident response policy and procedures, ensure those policies and procedures incorporates guidance from the privacy office for the handling of incidents involving personally identifiable information (PII).
Discussion for systems processing, storing, or transmitting PHI:
In developing incident response policy and procedures, ensure those policies and procedures incorporates guidance from the privacy office for the handling of incidents involving PHI.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
Applicable personnel (item a) include the Incident Response Team as required by OMB M-17-12.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
IR-02	**Incident Response Training**	**P2**	**Low** **Moderate** **High**

Control Statement

(a) Provide incident response training to system users consistent with assigned roles and responsibilities:
1. Within one (1) month of assuming an incident response role or responsibility or acquiring system access;
2. When required by system changes; and
3. Within every three hundred sixty-five (365) days thereafter; and

(b) Review and update incident response training content within every three hundred sixty-five (365) days and following defined events/incidents (specified in applicable system security and privacy plan).

Discussion

Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of AT-2 or AT-3. Events that may precipitate an update to incident response training content include, but are not limited to, incident response plan testing or

response to an actual incident (lessons learned), assessment or audit findings, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.	
Implementation Standard High, Moderate & Low: Std.1 - Formally tracks personnel participating in incident response training.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
AT-2, AT-3, AT-4, CP-3, IR-3, IR-4, IR-8, IR-9.
(Redacted Privacy Controls: AR-5)
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-5, AS-2;
	HIPAA: 45 C.F.R. §164.308(a)(6)(i);
	NIST SP: 800-16, 800-50;
	OMB Memo: M-16-04, M-19-03;

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): Those responsible for identifying and responding to a security incident must understand how to recognize sensitive information such as personally identifiable information (PII) or protected health information (PHI) is involved so that they can coordinate with the designated (e.g., privacy) official.	
Privacy Implementation Standards Systems processing, storing, or transmitting PII (to include PHI): PRIV.1 - Incident response training must include privacy education and awareness training associated with sending PII in email, identifying new privacy risks, mitigating privacy risks, and how and when to report privacy incidents and breaches.	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **IR-02(01)**	**Control Name** **Simulated Events**	**Priority** **P2**	**CMS Baseline** **High**
Control Statement Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.			
Discussion Organizations establish requirements for responding to incidents in incident response plans. Incorporating simulated events into incident response training helps to ensure that personnel understand their individual responsibilities and what specific actions to take in crisis situations. Incident response training includes tabletop exercises that simulate a breach. See IR-2(3).			
Implementation Standard High: Std. 1- Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			

HVA Implementation Standard

Control Number
IR-02(02)

Control Name
Automated Training Environments

Priority
P2

CMS Baseline
High

Control Statement
Provide an incident response training environment using automated mechanisms.

Discussion
Automated mechanisms can provide a more thorough and realistic incident response training environment. This can be accomplished, for example, by providing more complete coverage of incident response issues; by selecting more realistic training scenarios and training environments; and by stressing the response capability.

Implementation Standard
High:
Std. 1- Provide an incident response training environment using automated mechanisms.

Control Review Frequency
Annually (365 Days)

Assessment Frequency
Annually (365 Days)

Related Controls
None;

Reference Policy

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number
IR-02(03)

Control Name
Breach

Priority

CMS Baseline
Moderate
High

Control Statement
Provide incident response training on how to identify and respond to a breach, including the process for reporting a breach in accordance with the HHS Policy and Plan for Preparing For and Responding To a Breach of Personally Identifiable Information (PII).

Discussion
For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes. The incident response training emphasizes the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, oral, and electronic. Incident response training includes tabletop exercises that simulate a breach. See IR-2(1).

Implementation Standard
Std.1 - Provide incident response training on how to identify and respond to a breach, including the process for reporting a breach in accordance with the HHS Policy and Plan for Preparing For and Responding To a Breach of Personally Identifiable Information (PII).

Control Review Frequency
Annually (365 Days)

Assessment Frequency
Three (3) Years

Related Controls
None;

Reference Policy
OMB M-17-12;
SP 800-50.

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **IR-03**	**Control Name** **Incident Response Testing**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**

Control Statement

Test the effectiveness of the incident response capability for the system within every three hundred sixty-five (365) days using appropriate CMS-defined tests (e.g., the use of checklists, walk-through, discussion-based exercises or tabletop exercises, simulations, and comprehensive exercises) to determine the incident response effectiveness, and document the results.

Discussion

Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

Implementation Standard

High & Moderate:

Std.1 - Incident response capability tests must exercise (or simulate exercise of) all organizational response capabilities annually. The organization's documented response to an actual historic incident may be used as part of an incident response capability test, and any response capabilities that were not exercised as part of the previous actual incident response activities must be additionally exercised (or simulated) as part of the test.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
CP-3, CP-4, IR-2, IR-4, IR-8, PM-14.
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-5, AS-2;
	HIPAA: 45 C.F.R. §164.308(a)(6)(i);
	NIST SP: 800-84, 800-115;
	OMB Memo: A-130, M-16-04, M-19-03;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **IR-03(02)**	**Control Name** **Coordination with Related Plans**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**

Control Statement

Coordinate incident response testing with organizational elements responsible for related plans.

Discussion

Organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

Implementation Standard

High & Moderate:

Std. 1 - Coordinate incident response testing with organizational elements responsible for related plans.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
None;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	OMB Memo: M-16-04, M-19-03;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **IR-04**	**Control Name** **Incident Handling**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement (a) Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; (b) Coordinate incident handling activities with contingency planning activities; (c) Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and (d) Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.			
Discussion Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations consider incident response as part of the definition, design, and development of mission and business processes and systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring; user or administrator reports; and reported supply chain events. An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices). Suspected security incidents include the receipt of suspicious email communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components. For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes.			
Implementation Standard ??? High, Moderate & Low ??? Std.1 - Document relevant information related to a security and privacy incident per the current CMS Incident Handling and Breach Notification Standard and Procedures. Std.2 - Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow a chain of custody for forensic evidence. Std.3 - Identify vulnerability exploited during a security and privacy incident. Implement safeguards to reduce risk and vulnerability exploit exposure, including isolating or disconnecting systems. Std.4 - Incident response activities, to include forensic malware analysis, is coordinated with the ISSO and the CCIC. Each organization's security operations center: (a) Is responsible for actions to reduce the risk that an information security and/or privacy incident will occur and to respond appropriately to each incident or breach; and (b) Maintains primary responsibility for incident detection, including internal security monitoring and analysis of network traffic and logs. Std.5 - Contact information for individuals with incident handling responsibilities must be maintained in the system Incident Response Plan. (a) Changes must be documented in the system Incident Response Plan within three (3) days of the change.			

Control Review Frequency Seventy-Two (72) Hours	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-6, IR-8, IR-10, PE-6, PL-2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7
(Redacted Privacy Controls: SE-2)
	Reference Policy
	Executive Order: 13587;
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-5, AS-2;
	HHS Policy for Rules of Behavior for Use of Information and IT Resources (2019);
	HIPAA: 45 C.F.R. §164.308(a)(6)(ii), 45 C.F.R. Part 164 Subpart D;
	NIST SP: 800-61, 800-86, 800-101, 800-150, 800-160 v2, 800-184;
	OMB Memo: M-16-04, M-19-03;
	IR 7559

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

A strategic, well-thought-out security incident response program will integrate with privacy incident and breach response where appropriate, with the two processes being mutually supportive. The organizational Privacy Incident and Breach Response Plan may be integrated with the organizational Incident Response Plan. The organization privacy incident and breach response capability must be able to demonstrate knowledge of handling privacy incident and breach response processes and procedures and evidence showing the plan is followed routinely while responding to privacy incidents and breaches.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
PRIV.1 - Provide an organized and effective response to handling privacy incidents and breaches in accordance with HHS and CMS Privacy Incident (and Breach) Response Plans

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
IR-04(01)	**Automated Incident Handling Processes**	**P1**	**Moderate** **High**

Control Statement

Support the incident handling process using automated mechanisms.

Discussion

Automated mechanisms supporting incident handling processes include online incident management systems; and tools that support the collection of live response data, full network packet capture, and forensic analysis.
Contact your CRA or the CCIC for the list of compliant formats. All information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Implementation Standard

High & Moderate: High:

Std.1 - Automated mechanisms support the exchange of incident handling information with the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal requirements;
(b) Incident handling information sources include systems, appliances, devices, services, and applications (including databases);

(c) Incident handling information sources that do not support the exchange of information with the CCIC must be documented in the applicable risk assessment and security plan; and (d) CCIC directed incident handling information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.2 - As required by CMS, raw audit records must be available in an unaltered format to the CCIC. Moderate: Std.1 - Automated mechanisms support the exchange of incident handling information with the CCIC: (a) Information is provided to the CCIC in a format compliant with CMS and Federal requirements; (b) Incident handling information sources include systems, appliances, devices, services, and applications (including databases). (c) Incident handling information sources that do not support the exchange of information with the CCIC must be documented in the applicable risk assessment and security plan; and (d) CCIC directed incident handling information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.2 - As required by CMS, raw audit records must be available in an unaltered format to the CCIC.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls None;	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **IR-04(02)**	**Control Name** **DYNAMIC RECONFIGURATION**	**Priority**	**CMS Baseline** **HVA**
Control Statement Include the following types of dynamic reconfiguration for CMS HVA systems as part of the incident response capability: changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways.			
Discussion Dynamic reconfiguration includes changes to router rules, access control lists, intrusion detection or prevention system parameters, and filter rules for guards or firewalls. Organizations may perform dynamic reconfiguration of systems to stop attacks, misdirect attackers, and isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include specific time frames for achieving the reconfiguration of systems in the definition of the reconfiguration capability, considering the potential need for rapid response to effectively address cyber threats.			
Implementation Standard High, Moderate & Low: Std. 1 - Include the following types of dynamic reconfiguration for CMS HVA systems as part of the incident response capability: changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls AC-2, AC-4, CM-2.		**Reference Policy** NIST SP 800-61 Rev 2, NIST SP 800-86, NIST SP 800-101,NIST SP 800-150, NIST SP 800-160 v2, NIST SP 800-184	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			

Include the following types of dynamic reconfiguration for MAC system components as part of the overall HVA incident response capability: Dynamic reconfiguration includes changes to router rules, access control lists, intrusion detection or prevention system parameters, and filter rules for guards or firewalls.
HVA Discussion The agency may dynamically change router rules, access control lists, intrusion detection or prevention system parameters, and filter rules for guards or firewalls. Organizations may also perform dynamic reconfiguration of HVAs to stop attacks, misdirect attackers, or to isolate HVA components, thus limiting the extent of the damage from breaches or compromises. The organization may also re-assign cyber defense responsibilities to personnel or operating centers to manage risks. Organizations should include time frames for achieving the reconfiguration of HVAs in the definition of the reconfiguration capability.
HVA Implementation Standard

Control Number **IR-04(04)**	**Control Name** **Information Correlation**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.			
Discussion Sometimes a threat event, for example, a hostile cyber-attack, can only be observed by bringing together information from different sources, including various reports and reporting procedures established by organizations.			
Implementation Standard High: Std. 1 - Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
None;
		Reference Policy
		NIST SP: 800-61r2;
		OMB Memo: M-16-04, M-19-03;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement The organization can improve threat identification timeliness by correlating incident information across the enterprise.			
HVA Discussion Correlation information must be protected at a level congruent with the highest level of information it contains (AU-9). Sometimes a threat event, for example, a hostile cyber-attack, can only be observed by bringing together information from different sources, including various reports and reporting procedures established by organizations.			
HVA Implementation Standard The organization should correlate incident information and individual incident responses across the enterprise to achieve an organization-wide perspective on incident awareness and response.			

Control Number **IR-04(06)**	**Control Name** **Insider Threats – Specific Capabilities**	**Priority** **P3**	**CMS Baseline** **Above Baseline**
Control Statement Implement an incident handling capability for incidents involving insider threats.			
Discussion Explicit focus on handling incidents involving insider threats provides additional emphasis on this type of threat and the need for specific incident handling capabilities to provide appropriate and timely responses.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	

Related Controls
None;
	Reference Policy
	IS2P2;
	HHS: Policy for Monitoring Employee Use of HHS IT Resources;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **IR-04(08)**	**Control Name** **Correlation with External Organizations**	**Priority**	**CMS Baseline** **HVA**
Control Statement Coordinate with HHS CSIRC, CISA, US-CERT and other identified organizations to correlate and share incident response information to achieve a cross-organization perspective on incident awareness and more effective incident responses.			
Discussion The coordination of incident information with external organizations, including mission or business partners, military or coalition partners, customers, and developers, can provide significant benefits. Cross-organizational coordination can serve as an important risk management capability. This capability allows organizations to leverage critical information from a variety of sources to effectively respond to information security-related incidents potentially affecting the organization's operations, assets, and individuals.			
Implementation Standard High, Moderate & Low: Std. 1 - Coordinate with HHS CSIRC, CISA, US-CERT and other identified organizations to correlate and share incident response information to achieve a cross-organization perspective on incident awareness and more effective incident responses.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls AU-16, PM-16.		**Reference Policy** OMB Circular A-130, NIST SP 800-61 Rev 2	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement (a) Coordinate with external organizations to correlate and share incident information to achieve a cross-organization perspective on incident awareness and more effective incident responses. (b) Incident response plans for HVAs must incorporate external interconnected entities to ensure collaboration and reporting of appropriate information.			
HVA Discussion A complete incident response program that addresses all aspects incident response management to include collaboration with external organizations is crucial in ensuring prompt and effective incident response. Incident response plans for HVA incorporate external interconnected entities to ensure collaboration and reporting of appropriate information. ISA/MOU/MOAs shall include incident response requirements and reporting timeframes for all entities that interoperate with the HVA in accordance with US-CERT incident handling and Federal Reporting requirements.			
HVA Implementation Standard			

Control Number **IR-04(10)**	**Control Name** **SUPPLY CHAIN COORDINATION**	**Priority**	**CMS Baseline** **HVA**
Control Statement Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.			
Discussion			
Implementation Standard			

High, Moderate & Low: Std. 1 - Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls CA-3, MA-2, SA-9, SR-8.	**Reference Policy**
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement The organization should coordinate incident handling activities involving HVA and HVA component-related supply chain events with other organizations involved in the supply chain.	
HVA Discussion Other organizations involved in supply chain activities include product developers, HVA system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include compromises or breaches that involve HVA components, information technology products, development processes or personnel, and distribution processes or warehousing facilities. Organizations should consider including processes for protecting and sharing incident information in information exchange agreements. Coordination activities include sharing security and/or privacy incident information to the provider of the HVA or HVA service or other organizations involved in the supply chain for the HVA or HVA components related to the incident.	
HVA Implementation Standard	

Control Number **IR-04(11)**	**Control Name** **Integrated Incident Response Team**	**Priority**	**CMS Baseline** **High**
Control Statement Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in a reasonable time period [CMS ODP TBD], as resources allow, upon discovery/notification.			
Discussion An integrated incident response team is a team of experts that assesses, documents, and responds to incidents so that organizational systems and networks can recover quickly and can implement the necessary controls to avoid future incidents. Incident response team personnel include forensic and malicious code analysts, tool developers, systems security engineers, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions. For some organizations the incident response team can be a cross organizational entity. An integrated incident response team facilitates information sharing and allows organizational personnel (e.g., developers, implementers, and operators), to leverage team knowledge of the threat and to implement defensive measures that enable organizations to deter intrusions more effectively. Moreover, integrated teams promote the rapid detection of intrusions, development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing cyber intelligence development. Integrated incident response teams are better able to identify adversary tactics, techniques, and procedures that are linked to the operations tempo or to specific missions and business functions, and to define responsive actions in a way that does not disrupt those missions and business functions. Incident response teams can be distributed within organizations to make the capability resilient.			
Implementation Standard High: Std.1 - Integrated incident response team must include the CCIC IMT, CCIC FMAT, CCIC SOC, CMS CDM, Chief Information Officer, Chief Privacy Officer or Senior Official for Privacy, among others. The CCIC provides oversight of information security and privacy, to include incident reporting, for each FISMA system operated by or on behalf of CMS.			
Control Review Frequency	**Assessment Frequency**		

Annually (365 Days)	Annually (365 Days)
Related Controls AT-3	**Reference Policy**
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **IR-04(12)**	**Control Name** **Malicious Code and Forensic Analysis**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Analyze malicious code and/or other residual artifacts remaining in the system after the incident.			
Discussion Analysis of malicious code and other residual artifacts of a security or privacy incident can give the organization insight into adversary tactics, techniques, and procedures. It can also indicate the identity or some defining characteristics of the adversary. Malicious code analysis can also help the organization develop responses to future incidents.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **IR-04(14)**	**Control Name** **Security Operations Center**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Establish and maintain a security operations center.			
Discussion A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The organization staffs the SOC with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers) and implements a combination of technical, management, and operational controls (including monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to threat and security-relevant event data from multiple sources. These sources include perimeter defenses, network devices (e.g., routers, switches), and endpoint agent data feeds. The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. A SOC capability can be obtained in a variety of ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such capability.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
IR-05	**Incident Monitoring**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

Track and document incidents.

Discussion

Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics; and evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring; incident reports; incident response teams; user complaints; supply chain partners; audit monitoring; physical access monitoring; and user and administrator reports.

Implementation Standard

High, Moderate & Low:

Std.1 - The organization provides incident and breach information in format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements as part of the Information Security Continuous Monitoring (ISCM) plan.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)
Related Controls	**Reference Policy**

AU-6, AU-7, IR-8, PE-6, PM-5, SC-5, SC-7, SI-3, SI-4, SI-7
(Redacted Privacy Control: SE-2)
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-5, AS-2;
	HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(6)(ii), 45 C.F.R. Part 164 Subpart D;
	NIST SP: 800-61, 800-137;
	OMB Memo: M-14-03, M-16-04, M-19-03, M-20-04;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Tracking and documenting security and privacy incidents enables the organization to respond more effectively and evaluate both individual incidents and trends across incidents over time.

Privacy Implementation Standards

HVA Control Statement

(a) Track and document incidents.

(b) HVA Systems must track, monitor, and report incidents in accordance with US-CERT “Federal Incident Notification Guidelines”.

(c) Monitor all interconnected traffic into and out of the HVA to detect threats, and abnormal or malicious communications

HVA Discussion

Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics. It also includes evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports.

HVA Implementation Standard

Control Number **IR-05(01)**	**Control Name** **Automated Tracking, Data Collection, and Analysis**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Track security and privacy incidents and collect and analyze incident information using automated mechanisms.			
Discussion Automated mechanisms for tracking incidents and for collecting and analyzing incident information include Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.			
Implementation Standard High: Std. 1 - Track security and privacy incidents and collect and analyze incident information using automated mechanisms.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls AU-7, IR-4		**Reference Policy** NIST SP: 800-137;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **IR-06**	**Control Name** **Incident Reporting**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement (a). Require personnel to report suspected incidents to the organizational incident response capability within one (1) hour of discovery/notification; and (b). Report incident information to the CMS IT Service Help Desk.			
Discussion The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.			
Implementation Standard High, Moderate & Low: Std.1 - Designated authorities must include the CCIC. The CCIC provides oversight of information security and privacy, to include incident reporting, for each FISMA system operated by or on behalf of CMS. Std.2 - Forward information system security, privacy, and supply chain incident to CMS IT Service Help Desk Std. 3 - Collect and make available supporting information on the suspected security, privacy, and supply chain incident using the CMS Incident Response Reporting Template			
Control Review Frequency 1 hour		**Assessment Frequency** Annually (365 Days)	

Related Controls
CM-6, CP-2, IR-4, IR-5, IR-8, IR-9.
(Redacted Privacy Control: SE-2)
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		FISCAM: AC-5, AS-2;	

	HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(6)(ii), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(i)(C), 45 C.F.R. Part 164 Subpart D;
	NIST SP: 800-61;
	OMB Memo: M-17-12, M-16-04, M-19-03;
	Web: HYPERLINK "https://www.us-cert.gov/" ;

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): Incidents involving personally identifiable information (PII) must be reported to the appropriate incident response center, e.g., US-CERT or Intelligence Community Security Coordination Center.	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **IR-06(01)**	**Control Name** **Automated Reporting**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Report incidents using automated mechanisms.			
Discussion Reporting recipients are as specified in IR-6b. Automated reporting mechanisms include email, posting on web sites, and automated incident response tools and programs.			
Implementation Standard High & Moderate: Std.1 - Contact CMS IT Service Help Desk and report incident.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
IR-7
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		NIST SP: 800-61;
		Web: HYPERLINK "https://www.us-cert.gov/" ;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **IR-06(03)**	**Control Name** **SUPPLY CHAIN COORDINATION**	**Priority**	**CMS Baseline** **Moderate** **High**
Control Statement Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.			
Discussion			

Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Entities that provide supply chain governance include the Federal Acquisition Security Council (FASC). Supply chain incidents include compromises or breaches that involve information technology products, system components, development processes or personnel, distribution processes, or warehousing facilities. Organizations determine the appropriate information to share and consider the value gained from informing external organizations about supply chain incidents, including the ability to improve processes or to identify the root cause of an incident.	
Implementation Standard High & Moderate: Std. 1 - Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls SR-8	**Reference Policy**
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **IR-07**	**Control Name** **Incident Response Assistance**	**Priority** **P3**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of security, privacy, and supply chain incidents.			
Discussion Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensics services or consumer redress services, when required.			
Implementation Standard High, Moderate & Low: Std.1 - The CCIC provides centralized coordination and assistance on information security and privacy incident/breach awareness and management for all information systems across the CMS enterprise.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
AT-2, AT-3, IR-4, IR-6, IR-8, PM-22, PM-26, SA-9, SI-18.
(Redacted Privacy Control: SE-2
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		FISCAM: AC-5, AS-2;
		HIPAA: 45 C.F.R. §164.308(a)(6)(ii), 45 C.F.R. §164.308(a)(6)(i);
		OMB Memo: A-130, M-16-04, M-19-03;
		IR 7559.	

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI):			

<table>
<tr><td>Incident response assistance for incidents involving PII may include use of the forensic, technical, policy, and legal expertise of the organization’s Information Assurance Officers/Managers, Privacy Officers, Legal Counsel, external or internal IT help desks, and the organization’s Computer Emergency Response Team (CERT), in investigating and remediating incidents.</td></tr>
<tr><td><b>Privacy Implementation Standards</b>
High, Moderate & Low:
Std.1 - The CCIC provides centralized coordination and assistance on information security and privacy incident/breach awareness and management for all information systems across the CMS enterprise.</td></tr>
<tr><td><b>HVA Control Statement</b></td></tr>
<tr><td><b>HVA Discussion</b></td></tr>
<tr><td><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>IR-07(01)</b></td><td><b>Control Name</b>
<b>Automation Support for Availability of Information and Support</b></td><td colspan="2"><b>Priority</b>
<b>P2</b></td><td><b>CMS Baseline</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="5"><b>Control Statement</b>
Increase the availability of incident response information and support using automated mechanisms.</td></tr>
<tr><td colspan="5"><b>Discussion</b>
Automated mechanisms can provide a push or pull capability for users to obtain incident response assistance. For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.</td></tr>
<tr><td colspan="5"><b>Implementation Standard</b>
High & Moderate:
Std. 1 - Increase the availability of incident response information [TBD - Types of incident response information available from CCIC] and support using automated mechanisms by: (a) TBD - describe the CCIC baseline approach here.</td></tr>
<tr><td colspan="3"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="3"><b>Related Controls</b>
None;</td><td colspan="2"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
OMB Memo: M-16-04, M-19-03;</td></tr>
<tr><td colspan="5"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="5"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="5"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="5"><b>HVA Discussion</b></td></tr>
<tr><td colspan="5"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>IR-08</b></td><td><b>Control Name</b>
<b>Incident Response Plan</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
(a). Develop an incident response plan that:
1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;</td></tr>
</table>

3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
8. Is reviewed and approved by applicable Business Owner at least annually; and
9. Explicitly designates responsibility for incident response to applicable CMS Information System Security Officer (ISSO), approved by Business Owner.

(b). Distribute copies of the incident response plan to:

- CMS Chief Information Security Officer;
- CMS Chief Information Officer;
- CMS Information System Security Officer;
- CMS Cyber Risk Advisor (CRA);
- CMS Office of the Inspector General/Computer Crimes Unit;
- All personnel within CMS Incident Management/Response Team;
- All personnel within the PII Breach Response Team; and
- All personnel within the organization Operations Centers.

(c). Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;
(d). Communicate incident response plan changes to organizational elements listed in b. above; and
(e). Protect the incident response plan from unauthorized disclosure and modification.
(f). Review and update the IR Plan at a minimum every 365 days or when an IR event(s) demonstrates a change and/or update is needed to improve the IR Plan.

Discussion

It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions and business functions help determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information, include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

Implementation Standard

High, Moderate & Low:
Std. 1 - The system will a). Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
8. Is reviewed and approved by applicable Business Owner at least annually; and
9. Explicitly designates responsibility for incident response to applicable CMS Information System Security Officer (ISSO), approved by Business Owner.

(b). Distribute copies of the incident response plan to:

- CMS Chief Information Security Officer;
- CMS Chief Information Officer;
- CMS Information System Security Officer;
- CMS Cyber Risk Advisor (CRA);
- CMS Office of the Inspector General/Computer Crimes Unit;
- All personnel within CMS Incident Management/Response Team;
- All personnel within the PII Breach Response Team; and

- All personnel within the organization Operations Centers.

(c). Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;
(d). Communicate incident response plan changes to organizational elements listed in b. above; and
(e). Protect the incident response plan from unauthorized disclosure and modification. (f). Review and update the IR Plan at a minimum every 365 days or when an IR event(s) demonstrates a change and/or update is needed to improve the IR Plan.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls AC-2, CP-2, CP-4, IR-4, IR-7, IR-9, MP-2, MP-4, MP-5, PE-6, PL-2, SA-15, SI-12, SR-8. (Redacted Privacy Control: SE-2)	**Reference Policy** FedRAMP: Rev. 4 Baseline; HIPAA: 45 C.F.R. §164.308(a)(6) C.F.R.; NIST SP: 800-61; OMB A-130, M-17-12

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
Incorporates guidance from the Privacy Office for the handling of incidents involving personally identifiable information (PII) in the development of an incident response plan.
The organization Privacy Incident Response Plan is developed under the leadership of the Senior Official for Privacy (SOP). The plan includes:
(i)The establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan;
(ii)A process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly;
(iii)A privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks;
(iv)Internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to the SOP and other designated officials consistent with organizational incident management structures; and
(v)Internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials. Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a breach.
Organizations may also choose to integrate Privacy Incident Response Plans with Security Incident Response Plans or keep the plans separate.
Guidance for systems processing, storing, or transmitting PHI:
In developing an incident response plan, ensure it incorporates guidance from the privacy office for the handling of incidents involving PHI.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
PRIV.1 - Develops and implements a Privacy Incident and Breach Response Plan

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
IR-08(01)	**Breaches**		**Moderate** **High**

Control Statement

Include the following in the Incident Response Plan for breaches involving personally identifiable information:
(a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
(b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
(c) Identification of applicable privacy requirements.

Discussion Organizations may be required by law, regulation, or policy to follow specific procedures relating to privacy breaches, including notice to individuals, affected organizations, and oversight bodies, standards of harm, and mitigation or other specific requirements.	
Implementation Standard High, Moderate & Low: Std. 1 - Process to determine if notice to individuals or other organizations, including oversight organizations, is needed; Std. 2 - A risk assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and Std. 3 - Identification of applicable privacy requirements that were potentially violated.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls PT-1, PT-2, PT-3, PT-5, PT-6, PT-8.	**Reference Policy**
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Maintenance

Control Number	Control Name	Priority	CMS Baseline
MA-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel and roles:
   1. CMS Enterprise-level maintenance policy that:
      a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;
(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the maintenance policy and procedures; and
(c) Review and update the current maintenance:
   1. Policy at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
   2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

Maintenance policy and procedures address the controls in the MA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of maintenance policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to maintenance policy and procedures assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise level maintenance policy within this ARS, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures.)

Implementation Standard

High, Moderate & Low:
Std.1 - The CIO and CISO will provide leadership and oversight to develop, document, and disseminate to applicable stakeholder personnel and roles via the IS2P2:
   1. CMS Enterprise-level maintenance policy that:
      a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;
(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the maintenance policy and procedures; and
(c) Review and update the current maintenance:
   1. Policy at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and

2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
PM-9, PS-8, SI-12;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-1, SM-3;
	HIPAA: 45 C.F.R. §164.310(a)(2)(iv), 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.310(a)(2)(iii), 45 C.F.R. §164.310(d)(2)(iii);
	NIST SP: 800-12, 800-30, 800-39, 800-100;
	OMB A-130

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
MA-02	**Controlled Maintenance**	**P2**	**Low** **Moderate** **High**

Control Statement

(a) Schedule, document, and review records of maintenance, repair, or replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
(b) Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;
(c) Require that applicable Business Owner (or designated personnel/role specified in the applicable security plan) explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;
(d) Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement;
(e) Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
(f) Include maintenance-related information (defined in the applicable security and privacy plan) in organizational maintenance records.

Discussion

Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations consider supply chain-related risks associated with replacement components for systems. For systems categorized as Moderate or High, maintenance records should include: (i) the date and time of maintenance; (ii) the name of the individual performing the maintenance; (iii) the name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed and replaced (including identification numbers, if applicable). For systems categorized as High, ensure automated mechanisms are employed to schedule, conduct, and document any maintenance and repairs as required. The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems.

Implementation Standard

High, Moderate & Low:
Std. 1 - Equipment must be sanitized in accordance with NIST SP 800-88, as amended.

Control Review Frequency	**Assessment Frequency**

Annually (365 Days)	Annually (365 Days)

Related Controls
CM-2, CM-3, CM-4, CM-5, CM-8, MA-3, MP-6, PE-16, SI-2, SR-3, SR-4, SR-11;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;
	HIPAA: 45 C.F.R. §164.310(a)(2)(iv), 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.310(a)(2)(iii), 45 C.F.R. §164.310(d)(2)(iii);
	IR 8023;
	OMB Circular: A-130;

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **MA-02(02)**	**Control Name** **Automated Maintenance Activities**	**Priority** **P2**	**CMS Baseline** **High**

Control Statement (a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using automated mechanisms; and (b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.
Discussion The use of automated mechanisms to manage and control system maintenance programs and activities helps to ensure the generation of timely, accurate, complete, and consistent maintenance records.
Implementation Standard High, Moderate & Low: Std.1 The [desktop contract] supporting the GFE desktop, FedRAMP IaaS/PaaS providers, and data center contractors will: (a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using automated mechanisms; and (b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls MA-3;	**Reference Policy** See Control MA-2.

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **MA-03**	**Control Name** **Maintenance Tools**	**Priority** **P3**	**CMS Baseline** **Moderate** **High**

Control Statement

(a) Approve, control, and monitor the use of system maintenance tools; and (b) Review previously approved system maintenance tools every thirty (30) days [monthly].	
Discussion Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for the approval of maintenance tools and how that approval is documented. A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers. The hardware and software components that support maintenance and are a part of the system (including the software implementing utilities such as “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch) are not addressed by maintenance tools.	
Implementation Standard High & Moderate: Std. 1 - Ensure all maintenance tools, with the capability of retaining information, are checked to ensure that information is not saved on the tool and that the tool is appropriately sanitized, using approved sanitization methods discussed in NIST SP 800-88, as amended.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
MA-2, MA-5, MP-6, PE-16;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;
	NIST SP: 800-88;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **MA-03(01)**	**Control Name** **Inspect Tools**	**Priority** **P3**	**CMS Baseline** **Moderate** **High**
Control Statement Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.			
Discussion Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor’s website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.			
Implementation Standard High & Moderate: Std. 1 - Perform an Inspection the maintenance tools used by maintenance personnel for improper or unauthorized modifications.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	
Related Controls SI-7;		**Reference Policy** FedRAMP: Rev. 4 Baseline;	

	NIST SP: 800-88;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **MA-03(02)**	**Control Name** **Inspect Media**	**Priority** **P3**	**CMS Baseline** **Moderate** **High**
Control Statement Check media containing diagnostic and test programs for malicious code before the media are used in the system.			
Discussion If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations determine that the media contains malicious code, the incident is handled consistent with organizational incident handling policies and procedures.			
Implementation Standard High & Moderate: Std. 1 - Perform a malware check using CMS approved malware software on the media containing diagnostic and test programs for malicious code before the media are used in the system.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
SI-3;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		NIST SP: 800-88;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **MA-03(03)**	**Control Name** **Prevent Unauthorized Removal**	**Priority** **P3**	**CMS Baseline** **Moderate** **High**
Control Statement Prevent the removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from the CMS CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility.			
Discussion Organizational information includes all information owned by organizations and any information provided to organizations for which the organizations serve as information stewards.			
Implementation Standard Std. 1 - Ensure all maintenance tools, with the capability of retaining information, are checked to ensure that information is not saved on the tool and that the tool is appropriately sanitized, using approved sanitization methods discussed in NIST SP 800-88, as amended.			

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
MP-6;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	NIST SP: 800-88;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **MA-03(04)**	**Control Name** **Restricted Tool Use**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Restrict the use of maintenance tools to authorized personnel only.			
Discussion Restricting the use of maintenance tools to only authorized personnel applies to systems that are used to carry out maintenance functions.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls AC-3, AC-5, AC-6.		**Reference Policy** See MA-3;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **MA-03(05)**	**Control Name** **Execution with Privilege**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Monitor the use of maintenance tools that execute with increased privilege.			
Discussion Maintenance tools that execute with increased system privilege can result in unauthorized access to organizational information and assets that would otherwise be inaccessible.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls AC-3, AC-6;		**Reference Policy** See MA-3;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **MA-03(06)**	**Control Name** **Software Updates and Patches**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Inspect maintenance tools to ensure the latest software updates and patches are installed.			
Discussion Maintenance tools using outdated and/or unpatched software can provide a threat vector for adversaries and result in a significant vulnerability for organizations.			
Implementation Standard			
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years		
Related Controls AC-3, AC-6;	**Reference Policy** See MA-3;		
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **MA-04**	**Control Name** **Nonlocal Maintenance**	**Priority** **P2**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement (a) Approve and monitor nonlocal maintenance and diagnostic activities; (b) Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system; (c) Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions; (d) Maintain records for nonlocal maintenance and diagnostic activities; and (e) Terminate session and network connections when nonlocal maintenance is completed.			
Discussion Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Strong authentication requires authenticators that are resistant to replay attacks and employ multi-factor authentication. Strong authenticators include PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished, in part, by other controls. [SP 800-63B] provides additional guidance on strong authentication and authenticators.			
Implementation Standard High, Moderate & Low: Std.1 - Authentication and authenticators used during nonlocal maintenance and must be in accordance with NIST SP 800-63 rev3 B. Std.2 - Media used during remote maintenance must be sanitized in accordance with NIST SP 800-88, as amended.			
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)		

Related Controls
AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FIPS: 140-2, 140-3, 197, 201, 201-2;
	FISCAM: AS-1, SM-7;		

	HIPAA: 45 C.F.R. §164.312(a)(2)(iv), 45 C.F.R. §164.312(d), 45 C.F.R. §164.312(e)(1), 45 C.F.R. §164.312(e)(2)(ii);
	NIST SP: 800-63-3, 800-88;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **MA-04(03)**	**Control Name** **Comparable Security and Sanitization**	**Priority** **P2**	**CMS Baseline** **High**
Control Statement (a) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or (b) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.			
Discussion Comparable security capability on systems, diagnostic tools, and equipment providing maintenance services implies that the implemented controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.			
Implementation Standard High, Moderate & Low: Std.1 - (a) Nonlocal maintenance and diagnostic services must be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or (b) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for any or all organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.			
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)		
Related Controls MA-3, MP-6, SA-12, SI-3, SI-7;	**Reference Policy** NIST SP: 800-63-3, 800-88;		
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **MA-05**	**Control Name** **Maintenance Personnel**	**Priority** **P2**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement (a) Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel; (b) Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and			

(c) Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Discussion

Maintenance personnel refers to individuals performing hardware or software maintenance on organizational systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time-periods.

Implementation Standard

High, Moderate & Low:

Std.1 - (a) Establish a process for maintenance personnel authorization and maintain a list or log of authorized maintenance organizations or personnel;

(b) Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations and security credentials; and

(c) Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations following CMS established visitor logging and escort security protocols.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PE-4, PS-7, RA-3, SA-4;
(Redacted Privacy Controls: AR-3)
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;
	HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.310(a)(2)(iii), 45 C.F.R. §164.310(a)(2)(iv), 45 C.F.R. §164.310(d)(2)(iii);

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
MA-05(01)	**Individuals Without Appropriate Access**	**P2**	**High**

Control Statement

(a) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

(b) Develop and implement alternate controls (defined in applicable system security/privacy plan) in the event a system component cannot be sanitized, removed, or disconnected from the system.

Discussion

Procedures for individuals who lack appropriate security clearances or who are not U.S. citizens are intended to deny visual and electronic access to classified or controlled unclassified information contained on organizational systems. Procedures for the use of maintenance personnel can be documented in security plans for the systems.

Implementation Standard High, Moderate & Low: Std.1 - (a) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, i.e., foreign nationals, that include the following requirements: 1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted at all times and actively supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, possess the appropriate security credentials, and are technically qualified; 2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and (b) Develop and implement alternate mitigating controls (defined in applicable system security/privacy plan) in the event a system component cannot be sanitized, removed, or disconnected from the system.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)
Related Controls MP-6, PL-2;	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
MA-06	**Timely Maintenance**	**P2**	**Moderate** **High**

Control Statement Obtain maintenance support and/or spare parts for key information system components (defined in the applicable security and privacy plan) within the applicable Recovery Time Objective (RTO) specified in the system contingency plan.	
Discussion Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support include having appropriate contracts in place.	
Implementation Standard High, Moderate & Low: Std.1 - Obtain maintenance support and/or spare parts for key information system components (defined in the applicable security and privacy plan) as specified within the applicable Recovery Time Objective (RTO) detailed in the system contingency plan.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
CM-8, CP-2, CP-7, RA-7, SA-14, SA-15, SI-13, SR-2, SR-3, SR-4;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;
	HIPAA: 45 C.F.R. §164.310(a)(2)(iv)

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Media Protection

Control Number	Control Name	Priority	CMS Baseline
MP-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

a. Develop, document, and disseminate to applicable personnel and roles:
  1. CMS Enterprise-level media protection policy that:
    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
  2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;
b. Designates CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the media protection policy and procedures; and
c. Review and update the current media protection:
  1. Policy at least every three (3) years; and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
  2. Procedure at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

Media protection policy and procedures address the controls in the MP family that are implemented within systems and at the CMS Enterprise-level. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of media protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security or privacy incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise-level media protection policy within CMS IS2P2, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system-level security and privacy needs (i.e., special requirements that are unique to the CMS organization or system exist) are not fully addressed by the enterprise policy. (The implemented policy must not be less stringent than the enterprise policy and procedures).

Implementation Standard

High, Moderate & Low:

Std.1 - The CIO and CISO will provide leadership and oversight to:
(a) Develop, document, and disseminate to applicable personnel and roles:
  1. CMS Enterprise-level media protection policy that:
    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
  2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;
(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the media protection policy and procedures; and
(c) Review and update the current media protection:

1. Policy at least every three (3) years; and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and 2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls PM-9, PS-8, SI-12.	**Reference Policy** OMB A-130, NIST SP: 800-12, 800-30, 800-39, 800-100.
Privacy Discussion	
Privacy Implementation Standards Systems processing, storing, or transmitting PII (to include PHI): High, Moderate & Low: “Applicable personnel,” as referred to in MP-1(a), includes employees and contractors with potential access to personally identifiable information (PII).	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **MP-02**	**Control Name** **Media Access**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement The organization restricts access to digital and non-digital media pursuant to HHS Policy and in compliance with the latest revision of NIST SP 800-88, Guidelines for Media Sanitization to defined personnel or roles (defined in the applicable security and privacy plan).			
Discussion System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media.			
Implementation Standard High, Moderate & Low: Std.1 - Sensitive digital and non-digital media includes media containing personally identifiable information (PII). Std.2 - Sensitive digital and non-digital media includes media containing protected health information (PHI). Std.3 - Restrict access to sensitive digital and non-digital media pursuant to pursuant to HHS Policy, and in compliance with the latest version of NIST SP 800-88, Guidelines for Media Sanitization, to defined personnel or roles (defined in the applicable security plan) by disabling: (a) Disable CD/DVD writers and allow access to using CD/DVD viewing and downloading capabilities only to authorized individuals with a valid need to know. (b) Disable USB ports and allow access to using USB device capabilities only to authorized individuals with a valid need to know.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Annually (365 Days)	

Related Controls
AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SC-34, SI-12.
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		FIPS: 199;
		FISCAM: AC-4, AS-2;
		HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.310(c), 45 C.F.R. §164.310(d)(1);	

	NIST SP: 800-88, 800-111; OMB A-130.

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
Restricting access to digital and non-digital media, including mobile devices with storage capabilities, protects sensitive information, such as PII, from unauthorized use and disclosure. A risk assessment should be conducted to determine what sensitive information if any, can be stored on certain media types and who is authorized to do so.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
MP-03	**Media Marking**	**P2**	**Moderate** **High**

Control Statement

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempt defined types of system media, as specified, in writing, by the CMS CIO or his/her designated representative, from marking if the media remain within a secure environment.

Discussion

Security marking refers to the application or use of human-readable security attributes. Security labeling refers to the application or use of security attributes regarding internal data structures within systems. System media includes digital and non-digital media. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (solid state, magnetic), flash drives, compact disks, and digital versatile disks. Non-digital media includes paper and microfilm. Controlled unclassified information is defined by the National Archives and Records Administration along with the appropriate safeguarding and dissemination requirements for such information and is codified in [32 CFR 2002]. Security markings are generally not required for media that contains information determined by organizations to be in the public domain or to be publicly releasable. Some organizations may require markings for public information indicating that the information is publicly releasable. System media marking reflects applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Implementation Standard

High & Moderate:
Std.1 - (a) Stored data must have, at a minimum, the following data, clearly identifiable by labels or other approved coding systems:
a. The System Name
b. Creation Date
c. Sensitivity Classification (based on applicable record retention regulations)
d. CMS Contact Information.
(b) CMS CIO or his/her designated representative must specify in writing a specific media or hardware component exempted from marking if the media or hardware component remains within a secure environment.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)
Related Controls	**Reference Policy**
AC-16, CP-9, MP-5, PE-22, SI-12	EO 13556, 32 CFR 2002, FIPS 199.

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
Media containing personally identifiable information (PII) and protected health information (PHI), or the container for the media if labeling the media is not practicable, must be marked appropriately.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
MP-04	**Media Storage**	**P1**	**Moderate** **High**

Control Statement

The organization:

a. Physically controls and securely stores digital and non-digital media within CMS-controlled areas and data centers pursuant to HHS Policy; and

b. Protects system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Discussion

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (solid state, magnetic), compact disks, and digital versatile disks. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet; or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on organizations, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

Contact your CRA or the CCIC for the list of compliant formats.

Implementation Standard

High & Moderate:

Std.1 - Physically control and securely store digital and non-digital media defined in the latest revision of NIST SP 800-88, Guidelines for Media Sanitization, and HHS Policy, within CMS-controlled areas.

Std.2 - Ensure the protection of information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Std.3 - Provide secure storage in locked cabinets or safes for non-digital media.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)

Related Controls	Reference Policy

AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SC-34, SI-12.	FedRAMP: Rev. 4 Baseline;
	FIPS: 199;
	FISCAM: AC-4, AS-2;
	HIPAA: 45 C.F.R. §164.310(c), 45 C.F.R. §164.310(d)(1), 45 C.F.R. §164.310(d)(2)(iv);
	NIST SP: 800-56A, 800-56B, SP 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-88, 800-111;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Controlling the storage of media containing sensitive information such as PII protects the media from theft and promotes accountability.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - If PII is recorded on magnetic media with other data, the media should be protected as if all the data contained consisted of personally identifiable information.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
MP-05	**Media Transport**	**P1**	**Moderate** **High**

Control Statement

a. Protect and control digital and non-digital media pursuant to HHS Policy, as well as HHS Standards for Encryption of Computing Devices and Information, during transport outside of controlled areas using cryptography (in the case of sensitive information), and/or security safeguards (locked containers and tamper-evident packaging) commensurate with the FIPS 199 security categorizations for confidentiality and integrity of the data;
b. Maintain accountability for system media during transport outside of controlled areas;
c. Document activities associated with the transport of system media; and
d. Restrict the activities associated with the transport of system media to authorized personnel.

Discussion

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of system media in accordance with organizational assessments of risk. Organizations maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records.

Implementation Standard

High & Moderate:
Std.1 - Protect and control digital and non-digital media during transport outside of controlled areas using:
(a) Cryptography for media containing sensitive information; and
(b) Security safeguards locked containers and tamper-evident packaging.
Std.2 - Maintain accountability for all system media during transport outside of controlled areas.
Std.3 - Document activities associated with the transport of system media.
Std.4 - Restrict activities associated with the transport of CMS system media to authorized personnel.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)

Related Controls	Reference Policy
AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28, SC-34.	FIPS 199; NIST SP: 800-60-1, 800-60-2.

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
Protecting and controlling media containing sensitive information, such as PII, commensurate with the sensitivity of the information contained on the media, during transport outside of controlled areas, promotes accountability and limits situations that make the media vulnerable to unauthorized use and disclosure through loss, theft, or other mishandling.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
High & Moderate:
PRIV.1 - Protect and control non-digital PII/PHI media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. Non-digital PII must be in locked cabinets or sealed packing cartons while in transit.

HVA Control Statement

HVA Discussion
HVA Implementation Standard

Control Number **MP-05(03)**	**Control Name** **Custodians**	**Priority** **P3**	**CMS Baseline** **Above Baseline**
Control Statement Employ an identified custodian during transport of system media outside of controlled areas.			
Discussion Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another if an unambiguous custodian is identified.			
Implementation Standard High, Moderate & Low: Std.1 - Employ an identified custodian during transport of system media outside of controlled areas.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None:		**Reference Policy** See Control MP-5;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **MP-06**	**Control Name** **Media Sanitization**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement a. Sanitize digital and non-digital system media pursuant to HHS Policy prior to disposal, release out of organizational control, or release for reuse using defined sanitization techniques and procedures (defined in the applicable security and privacy plan) in accordance with applicable federal and organizational standards and policies, namely the latest revision of NIST SP 800-88, Guidelines for Media Sanitization; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.			
Discussion Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media such as paper and microfilm. The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques - including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction - prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. NARA policies controls the sanitization process for controlled unclassified information.			
Implementation Standard High & Moderate: Std.1 - Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.			

Std.2 - Surplus equipment is stored securely while not in use, and disposed of or sanitized in accordance with NIST 800-88 when no longer required.
Low:
Std.1 - Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11.
(Redacted Privacy Control: DM-2)
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FIPS: 199;
	FISCAM: AC-4, AS-2;
	HIPAA: 45 C.F.R. §164.310(d)(1), 45 C.F.R. §164.310(d)(2)(i), 45 C.F.R. §164.310(d)(2)(iii), 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.312(d)(2)(ii);
	32 CFR 2002;
	NIST SP: 800-60 v1, 800-60 v2, 800-88, 800-124;
	OMB A-130;
	IR 8023;
	NARA CUI;
	NSA MEDIA.

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
Properly sanitizing media that contains sensitive information, such as PII, prior to disposal or release protects the information from unauthorized use and disclosure.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
High, Moderate & Low:
PRIV.1 - Sanitize digital media that contains personally identifiable information (PII) prior to disposal, release out of organizational control, or release for reuse using FIPS-validated media sanitization techniques or procedures in accordance with applicable federal and organizational standards and policies.
PRIV.2 - Dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with a NARA approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.
PRIV.3 - Use FIPS-validated techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

HVA Control Statement

Provide proper sanitization mechanisms for HVA digital and non-digital media.

HVA Discussion

Media sanitization applies to all digital and non-digital HVA system media subject to disposal or reuse, whether or not the media is considered removable. Digital media include scanners, copiers, printers, notebook computers, workstations, network components, mobile devices. Non-digital media include paper and microfilm. The sanitization process removes information from HVA system media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, deidentification of personally identifiable information, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NARA policies control the sanitization.

HVA Implementation Standard

Std.1 - (a) Sanitize digital and non-digital system media that contains HVA data prior to disposal, release out of organizational control, or release for reuse using defined sanitization techniques and procedures (defined in the applicable security and privacy plan) in accordance with the latest revision of NIST SP 800-88, Guidelines for Media Sanitization, and HHS Policy, applicable federal and organizational standards and policies; and
(b) Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the HVA information contained within the media.

<table>
<tr><td><b>Control Number</b>
MP-06(01)</td><td><b>Control Name</b>
Review, Approve, Track, Document, and Verify</td><td><b>Priority</b>
P1</td><td><b>CMS Baseline</b>
High</td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Review, approve, track, document, and verify media sanitization and disposal actions.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking and documenting actions include listing personnel who reviewed and approved sanitization and disposal actions; types of media sanitized; files stored on the media; sanitization methods used; date and time of the sanitization actions; personnel who performed the sanitization; verification actions taken and personnel who performed the verification; and the disposal actions taken. Organizations verify that the sanitization of the media was effective prior to disposal.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High:
Std.1 - Ensure Personally Identifiable Information is securely destroyed or disposed of appropriately and reasonably and per retention schedules.
Std.2 - Review, approve, track, document, and verify media sanitization and disposal actions.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
None:</td><td colspan="2"><b>Reference Policy</b>
FIPS Pub: 199;
NIST SP: 800-60-1, 800-60-2, 800-88 800-124;
45 C.F.R. §164.310(d)(1); 45 C.F.R. §164.310(d)(2)(i); 45 C.F.R. §164.312(d)(2)(ii);
32 CFR 2002,
OMB A-130;
NARA CUI;
IR 8023,
NSA MEDIA.</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b>
Discussion for systems processing, storing, or transmitting PII (to include PHI):
Tracking, documenting, and verifying media sanitization and disposal actions for media that contains sensitive information, such as personally identifiable information (PII), reduces the risk of unauthorized disclosure of sensitive information and increases accountability.</td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
MP-06(02)</td><td><b>Control Name</b>
Equipment Testing</td><td><b>Priority</b>
P1</td><td><b>CMS Baseline</b>
High</td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Test sanitization equipment and procedures within every three hundred sixty-five (365) days to verify that the intended sanitization is being achieved.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities, including federal agencies or external service providers.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High:
Std.1 - Test sanitization equipment and procedures within every three hundred sixty-five (365) days to verify that the intended sanitization is being achieved.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
None:</td><td colspan="2"><b>Reference Policy</b>
FedRAMP Rev. 4 Baseline;</td></tr>
</table>

	FIPS Pub: 199;
	NIST SP: 800-60-1, 800-60-2, 800-88, 800-124;
	32 CFR 2002;
	OMB A-130;
	NARA CUI;
	IR 8023;
	NSA MEDIA

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
MP-06(03)	**Nondestructive Techniques**	**P1**	**High**

Control Statement Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: a. Prior to initial use after purchase; b. When obtained from an unknown source; c. When the organization loses a positive chain of custody; and d. When device was connected to a lower assurance network/system based on FIPS 199 security categorization.
Discussion Portable storage devices include external or removable hard disk drives (solid state, magnetic), optical discs, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks. Portable storage devices can be obtained from untrustworthy sources and can contain malicious code that can be inserted into or transferred to organizational systems through USB ports or other entry portals. While scanning storage devices is recommended, sanitization provides additional assurance that such devices are free of malicious code. Organizations consider nondestructive sanitization of portable storage devices when the devices are purchased from manufacturers or vendors prior to initial use or when organizations cannot maintain a positive chain of custody for the devices.
Implementation Standard High: Std.1 - Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system: (a)Prior to initial use after purchase; (b) When obtained from an unknown source; (c) When the organization loses a positive chain of custody; and (d) When device was connected to a lower assurance network/system based on FIPS 199 security categorization.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Annually (365 Days)

Related Controls
None:
	Reference Policy
	FIPS Pub: 199;
	NIST SP: 800-60-1, 800-60-2, 800-88, 800-124;
	32 CFR 2002;
	OMB A-130;
	NARA CUI;
	IR 8023;
	NSA MEDIA

Privacy Discussion	
Privacy Implementation Standards	

HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
MP-06(08)	**Remote Purging or Wiping of Information**	**P3**	**HVA**

Control Statement

The organization provides the capability to purge or wipe information from systems, system components, and devices either remotely or under CMS-defined conditions (defined in applicable system security and privacy plan).

Discussion

Remote purging or wiping of information protects information on organizational systems and system components if systems or components are obtained by unauthorized individuals. Remote purge or wipe commands require strong authentication to help mitigate the risk of unauthorized individuals purging or wiping the system, component, or device. The purge or wipe function can be implemented in a variety of ways, including by overwriting data or information multiple times or by destroying the key necessary to decrypt encrypted data.

Implementation Standard

High, Moderate & Low:

Std.1 - Provide the capability to purge or wipe information from systems, system components, and devices either remotely or under other defined conditions as defined in the applicable system security and privacy plan.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

None;
(Redacted Privacy Controls: DM-2, SE-2)
	FIPS Pub: 199;
	NIST SP: 800-60-1, 800-60-2, 800-88, 800-124;
	32 CFR 2002;
	OMB A-130;
	NARA CUI;
	IR 8023;
	NSA MEDIA;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Organizations must consider the use of this control for moderate and high personally identifiable information (PII) confidentiality impact level information on devices such as mobile devices like an iPad or other smart device. If your organization permits use of personal smart devices (for example, Bring Your Own Device [BYOD]), the organization must evaluate methods to ensure this control is enforced or that compensating controls are in place.

Privacy Implementation Standards

HVA Control Statement

Provide the capability to remotely purge or wipe information from HVA systems, system components, and devices in the event that the HVA or its component has been obtained by unauthorized individuals.

HVA Discussion

Remote purging or wiping of information protects information on the HVA system and component if either are obtained by unauthorized individuals. Remote purge or wipe commands require strong authentication to help mitigate the risk of unauthorized individuals purging or wiping the HVA system or component. The purge or wipe function can be implemented in a variety of ways, including by overwriting data or information multiple times or by destroying the key necessary to decrypt encrypted HVA data.

HVA Implementation Standard

Provide the capability to remotely purge or wipe information from HVA systems, components, and devices in the event that the HVA or its component has been obtained by unauthorized individuals.

Control Number	Control Name	Priority	CMS Baseline
MP-07	**Media Use**	**P1**	**Low** **Moderate** **High**

Control Statement

a. Prohibit the use of personally owned media (e.g. flash drives, external hard disk drives, other portable storage devices) on organization-defined systems or system components using defined security safeguards in accordance with CMS organizational policy and HHS IS2P; and
b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Discussion

System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, compact disks, digital versatile disks, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to MP-2, which restricts user access to media, MP-7 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations use technical and nontechnical controls to restrict the use of system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices, including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, such as by prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for storage devices reduces the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices.

Implementation Standard

High, Moderate & Low:
Std.1 - Prohibit the use of personally owned media such as flash drives, external hard disk drives, and other portable storage devices on organization-defined systems or system components.
Std.2 - Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)

Related Controls	Reference Policy

AC-19, AC-20, PL-4, PM-12, SC-34, SC-41
(Redacted Privacy Control: SE-2)
	FedRAMP Rev. 4 Baseline;
	FIPS: 199;
	HHS: IS2P 2014;
	NIST SP: 800-111

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
This control applies to devices containing PII, particularly portable storage and mobile devices.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
High, Moderate & Low:
PRIV. 1 - Prohibit the use of portable storage and mobile devices on information systems and networks containing personally identifiable information (PII), without using device ownership, media sanitization and encryption controls.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
MP-07(02)	**Prohibit Use of Sanitization-Resistant Media**		**Above Baseline**

Control Statement

Prohibit the use of sanitization-resistant media in organizational systems.

Discussion Sanitization resistance refers to how resistant media are to non-destructive sanitization techniques with respect to the capability to purge information from media. Certain types of media do not support sanitization commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitization-resistant media includes compact flash, embedded flash on boards and devices, solid state drives, and USB removable media.	
Implementation Standard	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years

Related Controls
MP-6
	Reference Policy
	FIPS 199;
	NIST SP: 800-111;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Physical and Environmental Protection

Control Number	Control Name	Priority	CMS Baseline
PE-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel:

1. CMS Enterprise-level physical and environmental protection policy that:
   a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

(c) Review and update the current physical and environmental protection:

1. Policy within every three (3) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures within every three (3) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines)

Discussion

Physical and environmental protection policy and procedures address the controls in the PE family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of physical and environmental protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to physical and environmental protection policy and procedures include assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise level physical and environmental protection policy within the CMS IS2P2, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures.)

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

AT-3, PM-9, PS-8, SI-12.;	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-1, SM-3;
	HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.310(a)(1), 45 C.F.R. §164.310(a)(2)(ii), 45 C.F.R. §164.310(a)(2)(iii);
	NIST SP: 800-12, 800-30, 800-39, 800-100;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

<table>
<tr><td>Control Number
PE-02</td><td>Control Name
Physical Access Authorizations</td><td>Priority
P1</td><td>CMS Baseline
Low
Moderate
High</td></tr>
<tr><td colspan="4">Control Statement
(a) Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;
(b) Issue authorization credentials for facility access;
(c) Review the access list detailing authorized facility access by individuals within every 90 days for High Systems, 180 days for Moderate Systems, and 365 days for Low Systems; and
(d) Remove individuals from the facility access list when access is no longer required.</td></tr>
<tr><td colspan="4">Discussion
Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.</td></tr>
<tr><td colspan="4">Implementation Standard</td></tr>
<tr><td colspan="2">Control Review Frequency
Annually (365 Days)</td><td colspan="2">Assessment Frequency
Three (3) Years</td></tr>
<tr><td colspan="2">Related Controls
AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PM-12, PS-3, PS-4, PS-5, PS-6.</td><td colspan="2">Reference Policy
Code: 5 U.S.C. §552a(b), (e)(10)164.310(a)(2)(iii);
Statute: Privacy Act of 1974 (P.L. 93-579);
FedRAMP: Rev. 4 Baseline;
FISCAM: AC-6, AS-2;
HIPAA: 45 C.F.R. §164.310(a)(1), 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.310(a)(2)(iii);
OMB Circular: A-130 7.g;
FIPS 201-2;
NIST SP: 800-73-4, 800-76-2, 800-78-4.</td></tr>
<tr><td colspan="4">Privacy Discussion</td></tr>
<tr><td colspan="4">Privacy Implementation Standards</td></tr>
<tr><td colspan="4">HVA Control Statement</td></tr>
<tr><td colspan="4">HVA Discussion</td></tr>
<tr><td colspan="4">HVA Implementation Standard</td></tr>
</table>

<table>
<tr><td>Control Number
PE-02(01)</td><td>Control Name
Access by Position or Role</td><td>Priority
P3</td><td>CMS Baseline
Above Baseline</td></tr>
<tr><td colspan="4">Control Statement
Authorize physical access to the facility where the system resides based on position or role.</td></tr>
<tr><td colspan="4">Discussion
Role-based facility access includes access by authorized permanent and regular/routine maintenance personnel, duty officers, and emergency medical staff.</td></tr>
<tr><td colspan="4">Implementation Standard</td></tr>
<tr><td colspan="2">Control Review Frequency
Not Specified</td><td colspan="2">Assessment Frequency
Three (3) Years</td></tr>
<tr><td colspan="2">Related Controls</td><td colspan="2">Reference Policy</td></tr>
</table>

AC-2, AC-3, AC-6;	HIPAA: 45 C.F.R. §164.310(a)(1), 45 C.F.R. §164.310(a)(2)(iii);
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **PE-03**	**Control Name** **Physical Access Control**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement (a) Enforce physical access authorizations at defined entry and exit points to the facility (defined in the applicable security and privacy plan) where the system resides by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress and egress to the facility using defined physical access control systems or devices and/or guards (defined in the applicable security and privacy plan); (b) Maintain physical access audit logs for defined entry or exit points (defined in the applicable security and privacy plan); (c) Control access to areas within the facility designated as publicly accessible by implementing defined security safeguards or physical access controls (defined in the applicable security and privacy plan) (d) Escort visitors and control visitor activity in defined circumstances requiring visitor escorts and controlling of visitor activity (defined in the applicable security and privacy plan); (e) Secure keys, combinations, and other physical access devices; (f) Inventory defined physical access devices (defined in the applicable security and privacy plan) every 90 days for High Systems and Moderate Systems, and 180 days for Low Systems; and (g) Change combinations and keys within every 365 days and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.			
Discussion Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas. Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.			
Implementation Standard High & Moderate: Std.1 - Control data center/facility access by use of door and window locks and security personnel or physical authentication devices, such as biometrics and/or smart card/PIN combination. Std.2 - Store and operate servers in physically secure environments and grant access to explicitly authorized personnel only. Access is monitored and recorded. Std.3 - Restrict access to grounds/facilities to authorized persons only. Low: Std.1 - Control data center/facility access by use of door and window locks. Std.2 - Store and operate servers in physically secure environments protected from unauthorized access.			
Control Review Frequency	**Assessment Frequency**		

Annually (365 Days)	Annually (365 Days)

Related Controls
AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.
	Reference Policy
	Code: 5 U.S.C. §552a(b) and (e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FIPS: 201, 201-2;
	FISCAM: AC-6, AS-2;
	HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.310(a)(1), 45 C.F.R. §164.310(a)(2)(iii), 45 C.F.R. §164.310(b), 45 C.F.R. §164.310(c);
	NIST SP: 800-73, 800-73-4, 800-76, 800-76-2, 800-78, 800-78-4, 800-116;
	OMB Circular: A-130 7.g;
	Web: HYPERLINK "https://www.idmanagement.gov/sell/fips201/" , HYPERLINK "https://www.idmanagement.gov/";

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a) Enforce physical access authorizations at defined entry and exit points to the facility (defined in the applicable security and privacy plan) where the HVA system resides by:

1. Verifying individual access authorizations before granting access to the facility;
2. Ensuring that physical access authorizations to HVA systems and environment must be authorized using dual authorizations; and
3. Controlling ingress and egress to the facility using defined physical access control systems or devices and/or guards (defined in the applicable security and privacy plan);

(b) Maintain physical access audit logs for defined entry or exit points (defined in the applicable security and privacy plan);
(c) Control access to areas within the facility designated as publicly accessible by implementing defined security safeguards or physical access controls (defined in the applicable security and privacy plan)
(d) Escort visitors and control visitor activity in defined circumstances requiring visitor escorts and controlling of visitor activity (defined in the applicable security and privacy plan);
(e) Secure keys, combinations, and other physical access devices;
(f) Inventory defined physical access devices (defined in the applicable security and privacy plan) every 90 days for High Systems and Moderate Systems, and 180 days for Low Systems; and
(g) Change combinations and keys within every 365 days and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.
(h) Physical access requests to HVA Systems must be reauthorized at least annually.

HVA Discussion

Physical access control applies to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Organizations should determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems requiring supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PE-03(01)	**System Access**	**P1**	**High** **HVA**

Control Statement

Enforce physical access authorizations to the system in addition to the physical access controls for the facility at defined physical spaces (defined in the applicable security and privacy plan) containing one or more components of the system.	
Discussion Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.	
Implementation Standard	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)
Related Controls	**Reference Policy** See Control PE-3;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Enforce physical access authorizations to the system in addition to the physical access controls for the facility at defined physical spaces (defined in the applicable security and privacy plan) containing one or more components of the system.	
HVA Discussion Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.	
HVA Implementation Standard	

Control Number **PE-04**	**Control Name** **Access Control for Transmission**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Control physical access to defined system distribution and transmission lines within organizational facilities using defined security controls or safeguards (defined in the applicable security and privacy plan).			
Discussion Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.			
Implementation Standard High & Moderate: Std.1 - Disable any physical ports (e.g., wiring closets, patch panels, etc.) not in use.			
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)		

Related Controls
AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-6, AS-2;
	HIPAA: 45 C.F.R. §164.310(a)(1), 45 C.F.R. §164.310(a)(2)(ii), 45 C.F.R. §164.310(c);		

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **PE-05**	**Control Name** **Access Control for Output Devices**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**
Control Statement Control physical access to output from defined output devices (in the applicable security and privacy plan) to prevent unauthorized individuals from obtaining the output.			
Discussion Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.			
Implementation Standard			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	

Related Controls
PE-2, PE-3, PE-4, PE-18;
		Reference Policy
		Code: 5 U.S.C. §552a(e)(10);
		Statute: Privacy Act of 1974 (P.L. 93-579);
		FedRAMP: Rev. 4 Baseline;
		FISCAM: AC-6, AS-2;
		HIPAA: 45 C.F.R. §164.310(a)(1), 45 C.F.R. §164.310(b), 164.310(c); OMB Circular: A-130 7.g;
		IR 8023	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **PE-06**	**Control Name** **Monitoring Physical Access**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement (a) Monitor physical access to the facility where the system resides to detect and respond to physical security incidents; (b) Review physical access logs weekly (every 7 days) and upon occurrence of defined events or potential indications of events (defined in the applicable security and privacy plan); and (c) Coordinate results of reviews and investigations with the organizational incident response capability.			
Discussion Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls, such as AU-2, if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.			
Implementation Standard			
Control Review Frequency Weekly		**Assessment Frequency** Annually (365 Days)	

Related Controls
AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-6, AS-2;
	HIPAA: 45 C.F.R. §164.310(a)(2)(iii), 45 C.F.R. §164.308(a)(6)(i);

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **PE-06(01)**	**Control Name** **Intrusion Alarms and Surveillance Equipment**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.			
Discussion Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and security guards by triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility.			
Implementation Standard			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	
Related Controls None;		**Reference Policy** FedRAMP: Rev. 4 Baseline;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **PE-06(04)**	**Control Name** **Monitoring Physical Access to Systems**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Monitor physical access to the system in addition to the physical access monitoring of the facility at defined physical spaces (defined in the applicable security and privacy plan) containing one or more components of the system.			
Discussion Monitoring physical access to systems provides additional monitoring for those areas within facilities where there is a concentration of system components, including server rooms, media storage areas, and communications centers. Physical access monitoring can be coordinated with intrusion detection systems and system monitoring capabilities to provide comprehensive and integrated threat coverage for the organization.			
Implementation Standard			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	
Related Controls PS-2, PS-3;		**Reference Policy** See Control PE-6;	
Privacy Discussion			

Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **PE-08**	**Control Name** **Visitor Access Records**	**Priority** **P3**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement (a) Maintain visitor access records to the facility where the system resides for two (2) years; (b) Review visitor access records no less often than monthly (every 30 days); and (c) Report anomalies in visitor access records to defined personnel or roles (defined in the applicable security and privacy plan).			
Discussion Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine if access authorizations are current and are still required to support organizational mission and business functions. Access records are not required for publicly accessible areas.			
Implementation Standard High, Moderate & Low: Std.1 - At a minimum, visitor access records must include the following information: 1. Name and organization of the person visiting; 2. Visitor’s signature; 3. Form of identification; 4. Date of access; 5. Time of entry and departure; 6. Purpose of visit; and 7. Name and organization of person visited.			

Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)
Related Controls PE-2, PE-3, PE-6;	**Reference Policy** None;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **PE-08(01)**	**Control Name** **Automated Records Maintenance and Review**	**Priority** **P3**	**CMS Baseline** **High**
Control Statement Maintain and review visitor access records using automated mechanisms (defined in the applicable security and privacy plan).			
Discussion			

Visitor access records may be stored and maintained in a database management system that is accessible by organizational personnel. Automated access to such records facilitates record reviews on a regular basis to determine if access authorizations are current and still required to support organizational mission and business functions.	
Implementation Standard	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)
Related Controls None;	**Reference Policy** See Control PE-8;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PE-09	**Power Equipment and Cabling**	**P1**	**Moderate** **High**

Control Statement Protect power equipment and power cabling for the system from damage and destruction.	
Discussion Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptable power sources in offices or data centers, generators and power cabling outside of buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.	
Implementation Standard High & Moderate: Std.1 - Permit only authorized maintenance personnel to access infrastructure assets, including power generators, heating, ventilation, and air conditioning (HVAC) systems, cabling, and wiring closets.	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls
PE-4;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PE-10	**Emergency Shutoff**	**P1**	**Moderate** **High**

Control Statement (a) Provide the capability of shutting off power to defined system or individual system components in emergency situations; (b) Place emergency shutoff switches or devices in defined location by system or system component (defined in the applicable security and privacy plan) to facilitate access for authorized personnel; and

(c) Protect emergency power shutoff capability from unauthorized activation.

Discussion
Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

Implementation Standard
High & Moderate:
Std.1 - Implements and maintains a main power switch or emergency cut-off switch, prominently marked and protected by a cover, for data centers, servers, and mainframe rooms.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
PE-15;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PE-11	**Emergency Power**	**P1**	**Moderate** **High**

Control Statement
Provide an uninterruptible power supply to facilitate an orderly shutdown of the system and/or transition of the system to long-term alternate power in the event of a primary power source loss.

Discussion
An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from unanticipated power interruptions from the main power source by providing energy stored in batteries, supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or properly shut down the system.

Implementation Standard

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls
AT-3, CP-2, CP-7;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **PE-11(01)**	**Control Name** **Alternate Power Supply - Minimal Operational Capability**	**Priority** **P1**	**CMS Baseline** **High**

Control Statement Provide an alternate power supply for the system that is activated manually and/or automatically and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.
Discussion Provision of an alternate power supply with minimal operating capability can be satisfied by accessing a secondary commercial power supply or other external power supply.
Implementation Standard High: Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements. Testing must comply with the previously mentioned recommendations, and be performed no less often than three (3) years.

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)
Related Controls None;	**Reference Policy** See Control PE-11;

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **PE-12**	**Control Name** **Emergency Lighting**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
Discussion The provision of emergency lighting applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Emergency lighting provisions for the system are described in the contingency plan for the organization. If emergency lighting for the system fails or cannot be provided, organizations consider alternate processing sites for power-related contingencies.
Implementation Standard High, Moderate & Low: Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements. Testing must comply with the previously mentioned recommendations, and be performed no less often than three (3) years.

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls
CP-2, CP-7;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion

HVA Implementation Standard

Control Number **PE-12(01)**	**Control Name** **Essential Missions and Business Functions**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Provide emergency lighting for all areas within the facility supporting essential mission and business functions.			
Discussion Organizations define their essential missions and functions			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **PE-13**	**Control Name** **Fire Protection**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement Employ and maintain fire detection and suppression systems that are supported by an independent energy source.			
Discussion The provision of fire detection and suppression systems applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.			
Implementation Standard High, Moderate & Low: Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements. Testing must comply with the previously mentioned recommendations, and be performed no less often than three (3) years.			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	

Related Controls
AT-3;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		FISCAM: AS-5, CP-2;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

<table>
<tr><td><b>Control Number</b>
<b>PE-13(01)</b></td><td><b>Control Name</b>
<b>Detection Systems - Automatic Activation and Notification</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Employ fire detection systems that activate automatically and notify defined personnel or roles (defined in the applicable security and privacy plan) and defined emergency responders (defined in the applicable security and privacy plan or safety plan) in the event of a fire.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g., to enter to facilities where access is restricted due to the classification or impact level of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Quarterly</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
None;</td><td colspan="2"><b>Reference Policy</b>
See Control PE-13;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>PE-13(02)</b></td><td><b>Control Name</b>
<b>Suppression Systems - Automatic Activation and Notification</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
(a) Employ fire suppression systems that activate automatically and notify defined personnel or roles (defined in the applicable security and privacy plan) and defined emergency responders (defined in the applicable security and privacy plan or safety plan); and
(b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances (e.g., to enter to facilities where access is restricted due to the impact level or classification of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Quarterly</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
None;</td><td colspan="2"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>PE-14</b></td><td><b>Control Name</b>
<b>Environmental Controls</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
(a) Maintain temperature, humidity, pressure, and radiation levels within the facility where the system resides at acceptable vendor-specified levels; and
(b) Monitor environmental control levels within the defined frequency (defined in the applicable security and privacy plan).</td></tr>
<tr><td colspan="4"><b>Discussion</b>
The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g., data centers, mainframe computer rooms, and server rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organizational mission and business functions.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High & Moderate:
Std.1 - Evaluate the level of alert and follow prescribed guidelines for that alert level.
Std.2 - Alert component management of possible loss of service and/or media.
Std.3 - Report damage and provide remedial action. Implement contingency plan, if necessary.
Low:
Std.1 - Evaluate the level of alert and follow prescribed guidelines for that alert level.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Quarterly</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
AT-3, CP-2</td><td colspan="2"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
FISCAM: AS-5, CP-2;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>PE-15</b></td><td><b>Control Name</b>
<b>Water Damage Protection</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Protect the system from damage resulting from water leakage by providing main shutoff or isolation valves that are accessible, working properly, and known to key personnel.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of main shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High, Moderate & Low:
Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements, no less often than three (3) years.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Quarterly</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
</table>

Related Controls
AT-3, PE-10;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-5, CP-2;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **PE-15(01)**	**Control Name** **Automation Support**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Detect the presence of water near the system and alert defined personnel or roles (defined in the applicable security and privacy plan) using automated mechanisms.			
Discussion Automated mechanisms include notification systems, water detection sensors, and alarms.			
Implementation Standard High: Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements, no less often than three (3) years.			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	
Related Controls None;		**Reference Policy** See Control PE-15;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **PE-16**	**Control Name** **Delivery and Removal**	**Priority** **P2**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement (a) Authorize and control defined types of system components (defined in the applicable security and privacy plan) entering and exiting the facility; and (b) Maintain records of the system components.			
Discussion Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.			
Implementation Standard			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	

Related Controls
CM-3, CM-8, MA-2, MA-3, MP-5, PE-20, SR-2, SR-3, SR-4, SR-6.
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		FISCAM: AC-6, AS-2;	

Privacy Discussion			

Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **PE-17**	**Control Name** **Alternate Work Site**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**

Control Statement (a) Determine and document the alternate work sites (defined in the applicable security and privacy plan) allowed for use by employees; (b) Employ appropriate controls (defined in the applicable security and privacy plan) at alternate work sites: (c) Assess the effectiveness of controls at alternate work sites; and (d) Provide a means for employees to communicate with information security and privacy personnel in case of incidents.
Discussion Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.
Implementation Standard

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-17, AC-18, CP-7.
	Reference Policy
	FISCAM: AS-5, CP-2;
	FedRAMP: Rev. 4 Baseline;
	HIPAA: 45 C.F.R. §164.310(a)(2)(i);
	NIST SP: 800-46;
	OMB Memo: M-11-27, M-17-12 Att. 1 and Att. 4;

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **PE-18**	**Control Name** **Location of System Components**	**Priority** **P3**	**CMS Baseline** **High**

Control Statement Position system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
Discussion Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Organizations consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to organizational communications using wireless packet sniffers or microphones, or unauthorized disclosure of information.
Implementation Standard

Control Review Frequency	**Assessment Frequency**

Quarterly	Annually (365 Days)

Related Controls
CP-2, PE-5, PE-19, PE-20, RA-3.
	Reference Policy
	Code: 5 U.S.C. §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FISCAM: AS-5, CP-2;
	HIPAA: 45 C.F.R. §164.310(c), 45 C.F.R. §164.308(a)(3)(i);

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Planning

Control Number	Control Name	Priority	CMS Baseline
PL-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel:

1.CMS Enterprise-level planning policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the planning policy and procedures; and

(c) Review and update the current planning:

1. Policy within every three (3) years; and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and

2. Procedures within every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

Planning policy and procedures for the controls in the PL family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to planning policy and procedures include, but are not limited to, assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise level planning policy within the CMS IS2P2, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures).

Implementation Standard

High, Moderate & Low:

Std.1 - The CIO and CISO will provide leadership and oversight to: (a) Develop, document, and disseminate to applicable stakeholder personnel via the IS2P2:

1.CMS Enterprise-level planning policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the planning policy and procedures; and

(c) Review and update the current planning:

1. Policy within every three (3) years; and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and

2. Procedures within every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
PM-9, PS-8, SI-12.
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-1, SM-3;
	HIPAA: 45 C.F.R. §164.316(a), 45 C.F.R. §164.316(b)(1)(i), 45 C.F.R. §164.316(b)(2)(i), 45 C.F.R. §164.316(b)(2)(ii);
	HSPD: HSPD 7 J(35);
	OMB A-130;
	NIST SP: 800-12, 800-18, 800-30, 800-39, 800-100;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **PL-02**	**Control Name** **System Security and Privacy Plan**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**

Control Statement

(a) Develop security and privacy plans for the system that:
1. Are consistent with the organization’s enterprise architecture;
2. Explicitly define the constituent system components;
3. Describe the operational context of the system in terms of missions and business processes;
4. Identify the individuals that fulfill system roles and responsibilities;
5. Identify the information types processed, stored, and transmitted by the system;
6. Provide the security categorization of the system, including supporting rationale;
7. Describe any specific threats to the system that are of concern to the organization;
8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
10. Provide an overview of the security and privacy requirements for the system;
11. Identify any relevant control baselines or overlays, if applicable;
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
13. Include risk determinations for security and privacy architecture and design decisions;
14. Include security- and privacy-related activities affecting the system that require planning and coordination with defined individuals or groups (defined in applicable system security and privacy plans); and
15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

(b) Distribute copies of the plans and communicate subsequent changes to the plans to applicable stakeholders;
(c) Review the plans within every three hundred sixty-five (365) days;
(d) Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
(e) Protect the plans from unauthorized disclosure and modification.

Discussion

System security and privacy plans are scoped to the system and system components within the defined authorization boundary and contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. The plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control. The control documentation describes how system-specific and hybrid controls are implemented and the plans and expectations regarding the functionality of the system. System security and privacy plans can also be used in the design and development of systems in support of life cycle-based security and privacy engineering processes. System security and privacy plans are living documents that are updated and adapted throughout the system development life cycle (e.g., during capability determination, analysis of alternatives, requests for proposal, and design reviews). Section 2.1 describes the different types of requirements that are relevant to organizations during the system development life cycle and the relationship between requirements and controls.

Organizations may develop a single, integrated security and privacy plan or maintain separate plans. Security and privacy plans relate security and privacy requirements to a set of controls and control enhancements. The plans describe how the controls and control enhancements meet the security and privacy requirements but do not provide detailed, technical descriptions of the design or implementation of the controls and control enhancements. Security and privacy plans contain sufficient information (including specifications of control parameter values for selection and assignment operations explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented.

Security and privacy plans need not be single documents. The plans can be a collection of various documents, including documents that already exist. Effective security and privacy plans make extensive use of references to policies, procedures, and additional documents, including design and implementation specifications where more detailed information can be obtained. The use of references helps reduce the documentation associated with security and privacy programs and maintains the security- and privacy-related information in other established management and operational areas, including enterprise architecture, system development life cycle, systems engineering, and acquisition. Security and privacy plans need not contain detailed contingency plan or incident response plan information but can instead provide—explicitly or by reference—sufficient information to define what needs to be accomplished by those plans.

Security- and privacy-related activities that may require coordination and planning with other individuals or groups within the organization include assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing. Planning and coordination include emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security- and privacy-related activities can also be included in other documents, as appropriate.

All CMS information systems and major applications are covered by a security and privacy plan, which is compliant with current CMS procedures. CFACTS is the CMS Governance, Risk and Compliance tool used as a repository to manage the security and privacy requirements of its information systems. This platform provides a common foundation to manage policies, controls, risks, assessments and deficiencies across the CMS Enterprise. Note: These stakeholders, groups, or organizations could include those involved with security-related activities, or providing services or support (such as TIC, or those involved in COOP planning). Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and CP/ITCP testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or non-urgent unplanned) situations.

Implementation Standard

High, Moderate & Low:

Std. 1 - All CMS information systems must develop and maintain a System Security and Privacy Plan compliant with current CMS guidelines, consistent with the CMS Technical Reference Architecture (TRA), and tracked by the CMS Federal Information Security Modernization Act Controls Tracking System (CFACTS) tool. The Authorizing Official (AO) must authorize a system to operate.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CM-13, CP-2, CP-4, IR-4, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PL-8, PL-10, PL-11, PM-1, PM-4, PM-7, PM-8, PM-9, PM-10, PM-11, RA-3, RA-8, RA-9, SA-5, SA-17, SA-22, SI-12, SR-2, SR-4.
	Reference Policy
	Statute: E-Government Act of 2002 (Pub. L. No. 107-347) §208; FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-1;
	HIPAA: 45 C.F.R. §164.306(a), 45 C.F.R. §164.308(a)(1)(i), 45 C.F.R. §164.310, 45 C.F.R. §164.310(a)(2)(ii), 45 C.F.R. §164.316(a), 45 C.F.R. §164.316(b)(1)(i), 45 C.F.R. §164.316(b)(2)(ii);
	HSPD: HSPD 7 J(35);
	NIST SP: 800-18; 800-37, 800-160 v1, 800-160 v2;
	OMB A-130, Appendix II;
	OMB Memo: M-03-22, M-17-12 Att. 1, A.2;

Privacy Discussion

Privacy Implementation Standards

Systems processing, storing, or transmitting PHI:
PHI.1 - Retain documentation of policies and procedures relating to HIPAA 164.306 for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b)).

HVA Control Statement

High & Moderate:
(a) Develop security and privacy plans for the HVA System must minimally include the following:

1. Security Categorization and supporting rationale;
2. Authorization boundary of the HVA;
3. Description of the HVA from a mission and business perspective;
4. Detailed description of the HVA operational environment;
5. Detailed interconnection information;
6. Description of the HVA protection needs;
7. Relevant overlays used (HVA, Privacy, etc.);
8. Control tailoring details and supporting rationale; and
9. Detailed description of the implementation of each control

(b) In accordance with CA-6(1), HVA Security and Privacy Plans are to be authorized and signed following the Joint Authorization method.
(c) Distribute copies of the plans and communicate subsequent changes to the plans to applicable stakeholders;
(d) Review the plans within every three hundred sixty-five (365) days;
(e) Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
(f) Protect the plans from unauthorized disclosure and modification.

HVA Discussion

Descriptions of tailored controls should include a detailed justification as to why the control was included or not and how it has been implemented. Control descriptions inherited from another system should also provide sufficient detail regarding how the control implementation meets control requirements for the HVA.
HVA Security and Privacy plans should include at least the following: Security Categorization and supporting rationale, authorization boundary of the HVA, description of the HVA from a mission and business perspective, detailed description of the HVA operational environment, detailed interconnection information, description of the HVA protection needs, relevant overlays used (e.g., HVA, Privacy, etc.), control tailoring details and supporting rationale, and detailed description of the implementation of each security control. In accordance with CA-6(1) as defined in this overlay, the HVA Security and Privacy Plan are to be authorized and signed following the Joint Authorization method.

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PL-04	**Rules of Behavior**	**P2**	**Low** **Moderate** **High**

Control Statement

(a) Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy including:
i. HHS Policy for Rules of Behavior (RoB) for Use of Information and IT Resources (2019); and
ii. Any applicable system-specific RoB.
(b) Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;
(c) Review and update the rules of behavior every three (3) years; and
(d) Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledged on an annual basis (at least every 365 days) or as needed, when the HHS RoB are revised or updated;

(e) Informs employees and contractors that the use of CMS information resources for anything other than authorized purposes set forth in the HHS RoB is a violation of either or both of those policies, and is grounds for disciplinary action, monetary fines, and/or criminal charges that could result in imprisonment.
(f) Informs employees and contractors that the use of CMS information resources is subject to the HHS Policy for Monitoring Employee Use of HHS IT Resources; and
(g) In addition to the HHS RoB, the organization may define a system-level RoB acknowledgement.

Discussion

Rules of behavior represent a type of access agreement for organizational users. Other types of access agreements include nondisclosure agreements, conflict-of-interest agreements, and acceptable use agreements (see PS-6). Organizations consider rules of behavior based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users, including individuals who receive information from federal systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for organizational and non-organizational users can also be established in AC-8. The related controls section provides a list of controls that are relevant to organizational rules of behavior. PL-4b, the documented acknowledgment portion of the control, may be satisfied by the literacy training and awareness and role-based training programs conducted by organizations if such training includes rules of behavior. Documented acknowledgements for rules of behavior include electronic or physical signatures and electronic agreement check boxes or radio buttons. Rules of behavior are aligned with HHS requirements and made readily available. HHS has established the HHS Rules of Behavior for Use of HHS Information and IT Resources available on the HHS intranet. Some OpDivs maintain their own OpDiv-level Rules of Behavior (RoB), which must be based upon the HHS RoB and no less restrictive. Usage of these RoBs is permissible as a substitute for the HHS RoB. In addition, a system-level RoB acknowledgement may also be required for some Moderate and High systems.

Implementation Standard

High, Moderate & Low:
Std. 1 - The organization must comply with the 'HHS Policy for Rules of Behavior for use of information and IT resources' incorporated in the annual Security and Privacy Awareness Training Computer Based Training (CBT) and all users must sign and submit a completed HHS ROB to there federal supervisor or contract administrator in charge of submitting Section F deliverables .

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, SI-12.
(Redacted Privacy Controls: AR-5)
	Code: 5 U.S.C. §552a(e)(9);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-4;
	HHS; Policy for Monitoring Employee Use of HHS IT Resources;
	HSPD: HSPD 7 J(35);
	NIST SP: 800-18;
	OMB Memo: M-17-12, Att. 1, A.2. and Att. 4;
	OMB A-130

Privacy Discussion

Rules of behavior govern expectations of system users for systems that handle sensitive information such as PII.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PL-04(01)	**Social Media and External Site / Application Usage Restrictions**	**P2**	**Low** **Moderate** **High**

Control Statement Include in the rules of behavior, restrictions on: (a) Use of social media, social networking sites, and external sites/applications; (b) Posting organizational information on public websites; and (c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.	
Discussion Social media, social networking, and external site/application usage restrictions address rules of behavior related to the use of social media, social networking, and external sites when organizational personnel are using such sites for official duties or in the conduct of official business, when organizational information is involved in social media and social networking transactions, and when personnel access social media and networking sites from organizational systems. Organizations also address specific rules that prevent unauthorized entities from obtaining non-public organizational information from social media and networking sites either directly or through inference. Non-public information includes personally identifiable information and system account information.	
Implementation Standard High, Moderate & Low: Std. 1 - All Enterprise personnel must comply with the 'HHS Policy for Rules of Behavior for use of information and IT resources' incorporated in the annual Security and Privacy Awareness Training Computer Based Training (CBT).	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AC-22, AU-13.
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	NIST SP: 800-18;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **PL-07**	**Control Name** **Concept of Operations**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement a. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and b. Review and update the CONOPS every three (3) years or whenever there is a major change.			
Discussion The CONOPS may be included in the security or privacy plans for the system or in other system development life cycle documents. The CONOPS is a living document that requires updating throughout the system development life cycle. For example, during system design reviews, the concept of operations is checked to ensure that it remains consistent with the design for controls, the system architecture, and the operational procedures. Changes to the CONOPS are reflected in ongoing updates to the security and privacy plans, security and privacy architectures, and other organizational documents, such as procurement specifications, system development life cycle documents, and systems engineering documents.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls PL-2, SA-2, SI-12.		**Reference Policy** OMB A-130	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			

HVA Discussion
HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PL-08	**Security and Privacy Architectures**	**P1**	**Moderate** **High** **HVA**

Control Statement

(a) Develop security and privacy architectures for the system that:

1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
3. Describe how the architectures are integrated into and support the enterprise architecture; and
4. Describe any assumptions about, and dependencies on, external systems and services;

(b) Review and update the architectures at least every three (3) years to reflect changes in the enterprise architecture; and

(c) Reflect planned architecture changes in the security and privacy plans, the Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

(d) Ensure that the planned architecture is consistent with the CMS's enterprise architecture program and is based on the taxonomy of the Federal Enterprise Architecture (FEA).

Note: Consult The Common Approach to Federal Enterprise Architecture and other for FEA guidance

Discussion

The security and privacy architectures at the system level are consistent with the organization-wide security and privacy architectures described in PM-7, which are integral to and developed as part of the enterprise architecture. The architectures include an architectural description, the allocation of security and privacy functionality (including controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The architectures can also include other information, such as user roles and the access privileges assigned to each role; security and privacy requirements; types of information processed, stored, and transmitted by the system; supply chain risk management requirements; restoration priorities of information and system services; and other protection needs.

[SP 800-160-1] provides guidance on the use of security architectures as part of the system development life cycle process. [OMB M-19-03] requires the use of the systems security engineering concepts described in [SP 800-160-1] for high value assets. Security and privacy architectures are reviewed and updated throughout the system development life cycle, from analysis of alternatives through review of the proposed architecture in the RFP responses to the design reviews before and during implementation (e.g., during preliminary design reviews and critical design reviews).

In today's modern computing architectures, it is becoming less common for organizations to control all information resources. There may be key dependencies on external information services and service providers. Describing such dependencies in the security and privacy architectures is necessary for developing a comprehensive mission and business protection strategy. Establishing, developing, documenting, and maintaining under configuration control a baseline configuration for organizational systems is critical to implementing and maintaining effective architectures. The development of the architectures is coordinated with the senior agency information security officer and the senior agency official for privacy to ensure that the controls needed to support security and privacy requirements are identified and effectively implemented. In many circumstances, there may be no distinction between the security and privacy architecture for a system. In other circumstances, security objectives may be adequately satisfied, but privacy objectives may only be partially satisfied by the security requirements. In these cases, consideration of the privacy requirements needed to achieve satisfaction will result in a distinct privacy architecture. The documentation, however, may simply reflect the combined architectures.

PL-8 is primarily directed at organizations to ensure that architectures are developed for the system and, moreover, that the architectures are integrated with or tightly coupled to the enterprise architecture. In contrast, SA-17 is primarily directed at the external information technology product and system developers and integrators. SA-17, which is complementary to PL-8, is selected when organizations outsource the development of systems or components to external entities and when there is a need to demonstrate consistency with the organization's enterprise architecture and security and privacy architectures. Consult The Common Approach to Federal Enterprise Architecture and other for FEA guidance.

Implementation Standard

High, Moderate & Low:

Std.1 - The CIO, CTO, SOP, and CISO will provide leadership and oversight to: (a) Develop security and privacy architectures under the Technical Reference Architecture (TRA) Volumes for the system that:

1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
3. Describe how the architectures are integrated into and support the enterprise architecture; and
4. Describe any assumptions about, and dependencies on, external systems and services;

(b) Review and update the architectures at least every three (3) years to reflect changes in the enterprise architecture; and

(c) Reflect planned architecture changes in the security and privacy plans, the Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

(d) Ensure that the planned architecture is consistent with the CMS's enterprise architecture program and is based on the taxonomy of the Federal Enterprise Architecture (FEA).

e) Deviations from the CMS approved TRA will require authorization and approval from the CMS Authorization Official (AO) as documented in the System Security and Privacy Plan (SSP) and may require a Risk Based Decision (RBD) via the Risk Acceptance process from the AO.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17, SC-7;
(Redacted Privacy Controls: AR-7)
	Reference Policy
	Code: 5 U.S.C. §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. 107-347) §208;
	FedRAMP: Rev. 4 Baseline;
	OMB Memo: M-03-22;
	OMB A-130;
	NIST SP: 800-160 v1, 800-160 v2

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a) Develop security and privacy architectures for the HVA system that:

1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
3. Describe how the architectures are integrated into and support the enterprise architecture; and
4. Describe any assumptions about, and dependencies on, external systems and services;

(b) Review and update the architectures at least every three (3) years to reflect changes in the enterprise architecture; and

(c) Reflect planned architecture changes in the security and privacy plans, the Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

(d) Ensure that the planned architecture is consistent with the CMS's enterprise architecture program and is based on the taxonomy of the Federal Enterprise Architecture (FEA).

HVA Discussion

In accordance with OMB M-19-03, organizations should ensure the following are being implemented: strict access control, multifactor authentication vulnerability scanning increased monitoring and analysis of events, network segmentation, boundary protections, and incident response testing.

The HVA security architecture should be designed and implemented in a layered approach based on risk assessment of threats to components and data, information flow, user access, insider threats, operational behaviors, and mission critical services.

Detailed data flows of information within the HVA should be developed and prioritized, and rules and policies should be created where segmentation and layers of isolation are identified. Devices that do not require direct access by HVA users should be located behind boundary protection devices with strict access control, filtering, and monitoring. Access lists should be set to default deny and permit by exception both inbound and outbound. Egress rules should block all access except required services and block all unnecessary traffic to the Internet. Security and administrative services and functions should be isolated onto their own networks with strict access control. The organization should implement access control lists to limit traffic between security, admin, and production networks. Traffic entering and leaving the HVA accreditation boundary should be encrypted in accordance with the risk analysis of the information being transmitted. Device services and applications should only be bound to the appropriate interface/network required for it to function.

HVA Implementation Standard

The organization should implement architectures designed to protect the security and privacy of the HVA and HVA data from potential compromise like external collocated systems and internal HVA components that are a higher risk posture (e.g., Internet facing systems).

Control Number **PL-08(01)**	**Control Name** **Defense-In-Depth**	**Priority**	**CMS Baseline** **HVA**
Control Statement Design the security and privacy architectures for the system using a defense-in-depth approach that: (a) Allocates HVA controls (defined in applicable security/privacy plans) to locations and architectural layers (defined in applicable security/privacy plans); and (b) Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.			
Discussion Organizations strategically allocate security and privacy controls in the security and privacy architectures so that adversaries must overcome multiple controls to achieve their objective. Requiring adversaries to defeat multiple controls makes it more difficult to attack information resources by increasing the work factor of the adversary; it also increases the likelihood of detection. The coordination of allocated controls is essential to ensure that an attack that involves one control does not create adverse, unintended consequences by interfering with other controls. Unintended consequences can include system lockout and cascading alarms. The placement of controls in systems and organizations is an important activity that requires thoughtful analysis. The value of organizational assets is an important consideration in providing additional layering. Defense-in-depth architectural approaches include modularity and layering (see SA-8(3)), separation of system and user functionality (see SC-2), and security function isolation (see SC-3).			
Implementation Standard High, Moderate & Low: Std.1 - The CIO and CISO will provide leadership and oversight to design the security and privacy architectures for the system using a defense-in-depth, i.e., multi-layered and dimensional security posture, approach that: (a) Allocates HVA controls (defined and specified in applicable security/privacy plans) to locations and architectural layers (defined in applicable security/privacy plans); and (b) Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	
Related Controls SC-2, SC-3, SC-29, SC-36.		**Reference Policy** OMB A-130; SP 800-160-1; SP 800-160-2	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Design the security and privacy architectures for the HVA system using a defense-in-depth approach that: (a) Allocates HVA-defined controls (defined in applicable security/privacy plans) to locations and architectural layers (defined in applicable security/privacy plans); and (b) Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.			
HVA Discussion Leveraging risk assessments, organizations protect information and mission critical services through a defense-in-depth approach for systems and information using multiple layers of security protections. Examples of the multiple layers are Web Zone, Application Zone, and Data Zone. Flow control and access control lists are implemented between layers using security safeguards, boundary protection devices, proxy servers, application gateways, intrusion prevention/detection etc. Figure 2, in HVA Control Overlay v2.0, depicts firewalls controlling access between the tiered layers. These firewalls are also used to monitor traffic for malicious content, unauthorized access, inside threats, and exfiltration.			
HVA Implementation Standard The organization should implement multiple layers of security boundaries to increase the security of HVA data and services.			

Control Number **PL-09**	**Control Name** **Central Management**	**Priority**	**CMS Baseline** **Moderate** **High**
Control Statement			

Centrally manage controls and related processes.	
Discussion Central management refers to organization-wide management and implementation of selected controls and processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of controls is generally associated with the concept of common (inherited) controls, such management promotes and facilitates standardization of control implementations and management and the judicious use of organizational resources. Centrally managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring. Automated tools (e.g., security information and event management tools or enterprise security monitoring and management tools) can improve the accuracy, consistency, and availability of information associated with centrally managed controls and processes. Automation can also provide data aggregation and data correlation capabilities; alerting mechanisms; and dashboards to support risk-based decision-making within the organization. As part of the control selection processes, organizations determine the controls that may be suitable for central management based on resources and capabilities. It is not always possible to centrally manage every aspect of a control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. The controls and control enhancements that are candidates for full or partial central management include but are not limited to: AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-4(all), AC-17(1), AC-17(2), AC-17(3), AC17(9), AC-18(1), AC-18(3), AC-18(4), AC-18(5), AC-19(4), AC-22, AC-23, AT-2(1), AT-2(2), AT-3(1), AT-3(2), AT-3(3), AT-4, AU-3, AU-6(1), AU-6(3), AU-6(5), AU-6(6), AU-6(9), AU-7(1), AU-7(2), AU11, AU-13, AU-16, CA-2(1), CA-2(2), CA-2(3), CA-3(1), CA-3(2), CA-3(3), CA-7(1), CA-9, CM-2(2), CM-3(1), CM-3(4), CM-4, CM-6, CM-6(1), CM-7(2), CM-7(4), CM-7(5), CM-8(all), CM-9(1), CM-10, CM-11, CP-7(all), CP-8(all), SC-43, SI-2, SI-3, SI-4(all), SI-7, SI-8.	
Implementation Standard High, Moderate & Low Std. 1 - All CMS systems must leverage the CFACTS tool as the standard governance tool for FISMA systems.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls PL-8, PM-9.	**Reference Policy** OMB A-130; NIST SP: 800-37
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PL-10	**Baseline Selection**		**Low** **Moderate** **High** **HVA**
Control Statement Select a control baseline for the system.			
Discussion Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (see PL-11). Federal control baselines are provided in [SP 800-53B]. The selection of a control baseline is determined by the needs of stakeholders. Stakeholder needs consider mission and business requirements as well as mandates imposed by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. For example, the control baselines in [SP 800-53B] are based on the requirements from [FISMA] and [PRIVACT]. The requirements, along with the NIST standards and guidelines implementing the legislation, direct organizations to select one of the control			

baselines after the reviewing the information types and the information that is processed, stored, and transmitted on the system; analyzing the potential adverse impact of the loss or compromise of the information or system on the organization's operations and assets, individuals, other organizations, or the Nation; and considering the results from system and organizational risk assessments. [CNSSI 1253] provides guidance on control baselines for national security systems.

Implementation Standard

High, Moderate & Low

Std. 1 - All CMS systems must leverage FIPS 199 system categorization process in CFACTS to select the initial set of baseline controls from NIST SP 800-53 Rev 5 and ARS 5.0.

Std. 2 - Organizations must adhere to the Baseline Selection requirements in NIST SP 800-53B.

Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years

Related Controls
PL-2, PL-11, RA-2, RA-3, SA-8.
	Reference Policy
	FIPS: 199, 200;
	NIST SP: 800-30, 800-37, 800-39, 800-53B, 800-60 v1, 800-60 v2, 800-160 v1;
	CNSSI 1253.

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

High and Moderate:

Select a control baseline for the HVA system.

HVA Discussion

Organizations should leverage FIPS 199 system categorization to select and tailor the initial baseline controls for HVA from NIST SP 800-53 Rev 5 (Moderate or High baselines only). All HVA systems should also implement the controls in the HVA overlay. Based on a risk assessment and the types of information stored, transmitted. And processed by the HVA, additional overlays may be necessary and other controls tailored in or out in accordance with the NIST Risk Management Framework.

HVA Implementation Standard

(a) The organization should implement at least the Moderate baseline from NIST SP 800-53 Rev 5. All HVA overlay controls should be applied as specified and not tailored.

(b) Additional controls for HVA systems should be applied in a risk-based manner in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and the Privacy Act to ensure sufficient security measures are implemented to protect HVAs.

Control Number	Control Name	Priority	CMS Baseline
PL-11	**Baseline Tailoring**		**Low** **Moderate** **High**

Control Statement

Tailor the selected control baseline by applying specified tailoring actions.

Discussion

The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific missions and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. Tailoring guidance is provided in [SP 800-53B]. Tailoring a control baseline is accomplished by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning values to control parameters; supplementing the control baseline with additional controls, as needed; and providing information for control implementation. The general tailoring actions in [SP 800-53B] can be supplemented with additional actions based on the needs of organizations. Tailoring actions can be applied to the baselines in [SP 800-53B] in accordance with the security and privacy requirements from [FISMA] and [PRIVACT]. Alternatively, other communities of interest adopting different control baselines can apply the tailoring actions in [SP 800-53B] to specialize or customize the controls that represent the specific needs and concerns of those entities.

Implementation Standard

High, Moderate & Low

Std. 1 - All CMS systems must leverage FIPS 199 system categorization to tailor any of the initial baseline controls from NIST SP 800-53 Rev 5 and ARS 5.0. Std. 2 - Organizations must adhere to the Baseline Tailoring requirements in NIST SP 800-53B.	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years

Related Controls
PL-10, RA-2, RA-3, RA-9, SA-8.
	Reference Policy
	FIPS: 199, 200;
	NIST SP: 800-30, 800-37, 800-39, 800-53B, 800-60 v1, 800-60 v2, 800-160 v1;
	CNSSI 1253.

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Program Management

Control Number **PM-01**	**Control Name** **Information Security Program Plan**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement

(a) Develops and disseminates a CMS Enterprise-wide, with supporting Mission/Business process-wide and System-wide (when needed), information security program plans that:

1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among CMS, CMS Mission/Business and System entities, and compliance;
3. Reflects coordination among CMS, CMS Mission/Business and System entities responsible for information security (i.e., technical, physical, personnel, cyber-physical); and
4. Is approved by a senior official with responsibility and accountability for the risk being incurred to CMS's organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.

(b) Review the CMS Enterprise-wide, with supporting Mission/Business/System-wide (when needed), information security program plans no less often than once every three hundred sixty-five (365) days and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and;

(c) Update the information security program plan at least every three hundred sixty-five (365) days and following CMS-defined events (e.g. assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines). to address organizational changes and problems identified during plan implementation or security control assessments; and

(d) Protect the information security program plan from unauthorized disclosure and modification.

Discussion

An information security program plan is a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. Information security program plans can be represented in single documents or compilations of documents. Privacy program plans and supply chain risk management plans are addressed separately in PM-18 and SR-2, respectively. Information security program plans documents implementation details about program management and common controls. The plans provide sufficient information about the controls (including specification of parameters for assignment and selection statements explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended. Updates to information security program plans include organizational changes and problems identified during plan implementation or control assessments.

Program management controls are generally implemented at the organization level and are essential for managing the organization's information security program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular system. The individual system security plans and the organization-wide information security program plan together, provide complete coverage for the security controls employed within the organization.

Common controls available for inheritance by organizational systems are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for a system. The organization-wide information security program plan indicates which separate security plans contain descriptions of common controls.

Events that may precipitate an update to the information security program plan include, but are not limited to, organization-wide assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines.

Implementation Standard

High, Moderate & Low:

Std.1 - Develop a CMS Enterprise-wide, with supporting Mission/Business process-wide and System-wide (when needed), information security program plans in the form of a CMS Information System Security and Privacy Policy (IS2P2) that outlines and establishes:

1. An overview of the requirements for the CMS information security and privacy program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
2. Identification and assignment of roles, responsibilities, management commitment, coordination among CMS, CMS Mission/Business and System entities, and compliance responsibilities;
3. Outline the coordination efforts required among CMS, CMS Mission/Business and System entities responsible for information security and privacy (i.e., technical, physical, personnel, cyber-physical); and
4. Publish an official CMS document that Is approved by the senior official, i.e., the CMS Authorization Official (AO) appointed, with responsibility and accountability for the risk being incurred to CMS's organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
PL-2, PM-8, PM-18, PM-12, RA-9, SI-12, SR-2, AR-2
	Reference Policy
	Code: 5 U.S.C. §552a, §552a(e)(10), 44 U.S.C. §3541, 44 U.S.C. §3506 (a)(3) and (g);
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347);
	HIPAA: 45 C.F.R. §164.308 (a)(1)(i), 45 C.F.R. §164.530(a)(1)(i), 45 C.F.R. §164.530(i)(1) - (3);
	OMB Circular: A-130 7.g.;
	OMB Memo: M-03-22, M-05-08, M-17-12;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
CMS’s approach to protection of personally identifiable information (PII) is to include protecting PHI in the information security program plan. This includes the definition of roles and responsibilities associated with protecting PII and any additional protections above the baseline PII requirements needed to be implemented necessary to meet PHI protection best practices or standards. As such, updates to the information security program plan must also address changes in federal privacy laws and policy requirements. Since CMS requires an annual review of the information security program plans, the statute driven requirement to review protecting PII as part of the privacy plan review (i.e., every two years) will be met.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PM-02	**Information Security Program Leadership Role**	**P1**	**Low** **Moderate** **High**

Control Statement

Appoints a CMS Chief Information Security Officer (CISO) with the mission and resources to coordinate, develop, implement, and maintain the CMS enterprise-wide information security program.

Discussion

The senior agency information security officer is an organizational official. For federal agencies (as defined by applicable laws, executive orders, regulations, directives, policies, and standards), this official is the senior agency information security officer. Organizations may also refer to this official as the senior information security officer or chief information security officer.

Implementation Standard

High, Moderate & Low:

Std.1 - Appoint a CMS Chief Information Security Officer (CISO) who supports the CMS Authorization Official (AO) with the mission and resources necessary to coordinate, develop, implement, and maintain the CMS enterprise-wide information security and privacy program.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
None;
	Reference Policy
	HIPAA: 45 C.F.R. §164.308(a)(2), 45 C.F.R. §164.530(a);
	NIST SP: 800-37, 800-39;
	OMB Memo: M-05-08, M-17-25;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PM-03	**Information Security and Privacy Resources**	**P1**	**Low** **Moderate** **High**
Control Statement (a) Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; (b) Prepare documentation (e.g., business case/Exhibit 300/Exhibit 53) required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and (c) Make available for expenditure, the planned information security and privacy resources.			
Discussion Organizations consider establishing champions for information security and privacy and as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board or similar group to manage and provide oversight for the information security and privacy aspects of the capital planning and investment control process.			
Implementation Standard High, Moderate & Low: Std.1 - The CMS Chief Information Security Officer (CISO) must: a) Identify and manage the resources needed to implement the information security and privacy programs via capital planning and investment requests and document all exceptions; (b) Prepare required documentation; business case/Exhibit 300/Exhibit 53 required for addressing information security and privacy programs in the CMS capital planning and investment request(s) process in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and (c) Prepare and make available for expenditure, the planned information security and privacy resources for program execution.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	

Related Controls
PM-4, SA-2;
		Reference Policy
		Statute: E-Government Act of 2002 (Pub. L. No. 107-347) §208;
		NIST SP: 800-65;
		OMB Circular: A-130;	

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI):			

To further accountability, plans, processes, and procedures associated with the Privacy Program plan (e.g., documenting the privacy requirements) are integrated into the Information Security Program plan. This combined format ensures both privacy and security controls are in place, or are planned for, to meet privacy requirements. This also enables the Information Security Program plan to serve both as evidence for CMS Business/System privacy operations and support resource requests supporting privacy.

A privacy-related portion of the combined and comprehensive Information Security Program plan should include a baseline listing of the selected privacy controls. It should also include:

(i) Processes for conducting privacy risk assessments (PIAs, PTAs. TPWAs);
(ii) Templates and guidance for completing PIAs, PTAs, PTWAs, and SORNs;
(iii) Privacy training and awareness requirements;
(iv) Requirements for contractors processing PII (to include PHI);
(v) Plans for eliminating unnecessary PII holdings; and
(vi) A framework for measuring annual performance goals and objectives for implementing identified privacy controls.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PM-04	**Plan of Action and Milestones Process**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Implement a process to ensure that Plans of Action and Milestones (POA&M) for the information security, privacy programs and supply chain risk management and associated CMS Mission/Business/Systems (CMS Plan of Action and Milestones Process Guide V 1.1 and HHS Plan of Action and Milestones Process Standard V 2.0):

1. Are developed and maintained;
2. Document the remedial information security, privacy and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
3. Are reported in accordance with established reporting requirements e.g. OMB FISMA reporting requirements and other applicable requirements, such as those within the Federal Risk and Authorization Management Program (FedRAMP).

(b) Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Discussion

The plan of action and milestones is a key organizational document and is subject to reporting requirements established by the Office of Management and Budget. Organizations develop plans of action and milestones with an organization-wide perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from control assessments and continuous monitoring activities. There can be multiple plans of action and milestones corresponding to the information system level, mission/business process level, and organizational/governance level. While plans of action and milestones are required for federal organizations, other types of organizations can help reduce risk by documenting and tracking planned remediations. Specific guidance on plans of action and milestones at the system level is provided in CA-5.

Implementation Standard

High, Moderate & Low:

Std.1 - The CMS FISMA governance tool (CMS FISMA Continuous Tracking System [CFACTS]) performs the following:

1. Document the remedial information security, privacy and supply chain risk management actions via the development of Plan of Action and Milestones (POA&M) to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
2. Report in accordance with established reporting requirements e.g. OMB FISMA reporting requirements and other applicable requirements, such as those within the Federal Risk and Authorization Management Program (FedRAMP) the vulnerabilities or weaknesses identified via security audits, security control assessments, and/or continuous monitoring activities; and

3. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. [CRA responsibility? TBD]

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
CA-5, CA-7, PM-3, RA-7, SI-12;
	Reference Policy
	Statute: Privacy Act of 1974 (P.L. 93-579);
	HIPAA: 45 C.F.R. §164.310(d);
	NIST SP: 800-37, 800-39, 800-137;
	OMB Circular: A-130;
	OMB Memo: M-02-01, M-14-03, M-16-04, M-19-03, M-20-04;
	HHS Standard for Plan of Action and Milestones (POAM) Management and Reporting
	CMS Plan of Action and Milestones Process Guide

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Since the security controls section of a privacy impact assessment, or other privacy documentation, may not provide sufficient detail to verify the effectiveness of implemented privacy-related security controls, review of system POA&Ms can be used to provide a snapshot on effectiveness of the controls.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PM-05	**System Inventory**	**P1**	**Low** **Moderate** **High**

Control Statement

Develop and update an inventory of organizational systems, to include those operated on behalf of CMS (e.g., by a contractor, vendor, cloud service provider, or other service provider) that does not exceed 30 days,

Note: The 30 day reporting window is required to support DHS CDM reporting requirements.

Discussion

OMB A-130 provides guidance on developing systems inventories and associated reporting requirements. This control refers to organization-wide inventory of systems, not system components as described in CM-8.

Implementation Standard

High, Moderate & Low:

Std.1 - The CMS Cybersecurity Integration Center (CCIC) will utilize automated tools to:

1. Produce an inventory of organizational systems, to include those operated on behalf of CMS (e.g., by a contractor, vendor, cloud service provider, or other service provider) that does not exceed 30 days in age.
2. Submit the inventory of organizational systems report to DHS CDM per requirements.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
CM-8, CM-12, CM-13, PL-8, PM-22, PT-3, PT-6, SI-12, SI-18;
	Reference Policy
	NISTIR: 8062;
	NIST SP: 800-137;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Maintaining an accurate and current system inventory supports privacy by: maintaining inventories of personally identifiable information (PII), identifying data flows associated with the movement of PII, and monitoring the maintenance and use of PII.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PM-05(01)	**Inventory of Personally Identifiable Information**	**P1**	**Moderate** **High**

Control Statement

Establish, maintain, and update at least annually an inventory of all systems, applications, and projects that process personally identifiable information to include any system processing protected health information.

Discussion

An inventory of systems, applications, and projects that process personally identifiable information supports mapping of data actions, providing individuals with privacy notices, maintaining accurate personally identifiable information, and limiting the processing of personally identifiable information when such information is not needed for operational purposes. Organizations may use this inventory to ensure that systems only process the personally identifiable information for authorized purposes and that this processing is still relevant and necessary for the purpose specified therein.

All CMS systems are required to perform an inventory of PII, even if no PII is processed, stored or transmitted by the system. This ensures that systems that do not process, store or transmit PII will include a statement to that effect in their documentation.

Implementation Standard

High, Moderate & Low:

Std. 1 - The CMS Cybersecurity Integration Center (CCIC) will utilize the CFACTS tool to:

1. Produce an inventory of all systems, applications, and projects that process personally identifiable information to include any system processing protected health information.
2. Make the PII/PHI inventory available upon request to security auditors and/or security control assessors.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years

Related Controls	Reference Policy

CM-8, CM-12, CM-13, PL-8, PM-22, PT-3, PT-6, SI-12, SI-18;	Code: 5 U.S.C. §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208(b)(2);
	FIPS: 199;
	HIPAA: 45 C.F.R. §164.530(c), 45 C.F.R. §164.310(d);
	NIST SP: 800-37r2, 800-122;
	OMB Circular: A-130 Appendix I;
	OMB Memo: M-03-22, M-16-04, M-17-12 Att. 1 & B.1.a;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

While all CMS systems are required to perform an inventory of PII, systems that do not process, store, or transmit PII are not required to forward the PII update to the CMS Senior Official for Privacy.

The PII inventory identifies the CMS Business/System information assets and identifies those assets collecting, using, maintaining, or sharing PII. The PII inventory identifies those assets most likely to impact privacy; provides a starting point for CMS Businesses/Systems to implement effective administrative, technical, and physical security policies and procedures to protect PII; and to mitigate risks of PII exposure.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Amend control to include:

(a) Provide each update of the PII inventory to the CMS Senior Official for Privacy and the CMS CISO no less often than once every three hundred sixty-five 365 days to support the establishment of information security requirements for all new or modified systems containing PII.
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **PM-06**	**Control Name** **Measures of Performance**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement Develop, monitor, and report on the results of information security and privacy measures of performance to evaluate the effectiveness of IT security and privacy policies, procedures, and controls. The measures and metrics must provide information on measures of implementation, efficiency, effectiveness, and impact.			
Discussion Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security and privacy programs and the controls employed in support of the program. To facilitate security and privacy risk management, organizations consider aligning measures of performance with the organizational risk tolerance as defined in the risk management strategy.			
Implementation Standard High, Moderate & Low: Std.1 - CMS establishes security program metrics via CFACTS and CDM tools utilized in the CCIC under the oversight of the Cyber Risk Management Program (CRMP) within the Information Security and Privacy Group (ISPG) - Division of Implementation and Reporting: • Cyber Risk Management Program (CRMP): Interprets mandates and regulations to develop metrics. These metrics are translated into reporting dashboards that define risk thresholds and allows CMS to identify issues quickly through continuous assessment of the controls and risk exposure. • Cyber Risk Reports (CRR): Communicates cyber risk metrics in a consistent manner across all Federal Information Security Management Act (FISMA) Systems. ISPG generates Cyber Risk Reports monthly to help Business Owners (BO) and System Owners make risk-based decisions at the system level.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	

Related Controls
CA-7;PM-9
		Reference Policy
		NIST SP: 800-55, 800-137;
		OMB Circular: A-130;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **PM-07**	**Control Name** **Enterprise Architecture**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.			
Discussion			

The integration of security and privacy requirements and controls into the enterprise architecture helps to ensure that security and privacy considerations are addressed throughout the system development life cycle and are explicitly related to the organization's mission and business processes. The process of security and privacy requirements integration also embeds into the enterprise architecture, the organization's security and privacy architectures consistent with the organizational risk management strategy. For PM-7, security and privacy architectures are developed at a system-of-systems level, representing all organizational systems. For PL-8, the security and privacy architectures are developed at a level representing an individual system. The system-level architectures are consistent with the security and privacy architectures defined for the organization. Security and privacy requirements and control integration are most effectively accomplished through the rigorous application of the Risk Management Framework (NIST SP 800-37) and supporting security standards and guidelines.

Implementation Standard

High, Moderate & Low:

Std.1 - CMS establishes a Technical Reference Architecture (TRA) under the oversight of the Chief Technology Officer (CTO), following the Federal Enterprise Architecture (FEA) guidelines to provide technical reference standards for all CMS production environments and future application designs, to ensure a secure and effective operating environment.

1 - Publish a series of TRA Volumes to outline and communicate CMS' technical architecture approach and describe the technical baseline to support system development and maintenance contracts for hosting CMS systems.

2 - Participate in and attend the HHS CIO and Federal CIO Council boards, share information with CMS stakeholders, and make adjustments to published architectural guidelines based on changing federal architectural mandates.

3 - Develop and publish a System Development Life Cycle (SDLC) that utilizes the CMS TRA to ensure that security considerations are addressed by CMS early in the SDLC and are directly and explicitly related to the CMS mission/business processes.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AU-6, PL-2, PL-8, PM-11, RA-2, SA-3, SA-8, SA-17, AR-7
	Reference Policy
	Code: 5 U.S.C. §552a, §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208(b) and §208(c);
	HIPAA: 45 C.F.R. §164.308(a)(1)(i), 45 C.F.R. §164.530(c);
	NIST SP: 800-37, 800-39, 800-160v1, 800-160v2;
	OMB Circular: A-130 7.g.;
	OMB Memo: M-03-22, M-17-12;
	OMB Report: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, Federal Trade Commission Final Report (March 2012);

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Automating privacy controls provides a concrete way of ensuring systems are behaving in a way that is intended to achieve privacy objectives. Implementation of this control enables CMS Businesses/Systems to automate application of privacy controls. One simple example, which many CMS Businesses/Systems have already implemented, is PT-6, "Privacy Notice." This concept is one part of the most commonly recognized approaches to "building privacy in," which is sometimes also known as "Privacy by Design." Privacy by Design is an internationally accepted privacy best practice endorsed by the Federal Trade Commission in their March 2012 Final Report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," and embodies the same principles of the Privacy Act and Section 208 of the E-Government Act requiring privacy protections and safeguards before establishing or operating a system that may contain PII. Privacy by Design calls for considering privacy risks in the design and management of systems. In addition to building in security and privacy controls discussed throughout the ARS, this control considers additional privacy-specific system characteristics and controls that must be built into the system to address privacy risks.

To the extent feasible, when designing CMS Business/System systems, technologies and system capabilities are employed that automate privacy controls on the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, CMS Businesses/Systems mitigate privacy risks to PII, thereby reducing the likelihood of system breaches and other privacy-related incidents.

CMS Businesses/Systems also conduct periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act and CMS's privacy policy. Regardless of whether automated privacy controls are employed, CMS Businesses/Systems regularly monitor system use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notices from CMS Businesses/Systems, or in a manner compatible with those purposes. Additional guidance on privacy-enhanced design and development may be found in the HHS Enterprise Performance Lifecycle (EPLC).

Regardless of the systems engineering lifecycle used, privacy requirements should be considered during system design and development and validated and verified along with other system requirements. Validation ensures the correct requirements were identified. Verification ensures the requirements were implemented correctly.
Reference the FEA Security and Privacy Profile for additional information.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
High & Moderate:
PRIV.1 - Amend control to include:

(a) Design the systems to support privacy by automating privacy controls to the greatest extent feasible, integrating and meeting CMS's privacy requirements throughout the system's Life Cycle, and incorporating privacy concerns into all reviews for significant changes to CMS systems, networks, physical environments, and other agency-related infrastructures.

(b) Include the need for updates to maintain compliance with the Privacy Act, CMS's and the Mission's/Business's/System’s privacy policy, and any other legal or regulatory requirements within all system reviews.

HVA Control Statement

Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational HVA operations and assets, individuals, other organizations, and the Nation.

HVA Discussion

The dependency of the HVAs on the enterprise mandates the integration of security requirements and controls into the Enterprise Architecture (EA) to ensure HVAs are adequately protected by the enterprise to ensure the critical business functions and mission of the organization. The enterprise is considered a large and complex system, or system of systems. The EA should align business and technology resources to achieve strategic outcomes. agencies should develop an EA that describes the baseline architecture, target architecture, and transition plan to get to the target architecture while considering organizational risk management, effective security control implementation, and if necessary, privacy strategies.

The EA should be implemented, enforced, and executed at levels 1 and 2: Organization (level 1), mission/business (level 2) but must facilitate and support the functions and solutions at the System or component level (level 3). The EA should also incorporate agency plans for significant upgrades or replacements of legacy applications, systems, or solutions that are too costly to operate, maintain, and secure. The EA should include plans for disposition of applications, systems, or solutions when no longer effectively support missions or business functions as well as strategies for interacting and connecting to external systems and environments (cloud, hosting providers, other government entities, contractor facilities.

As organizations develop plans for transitioning from current operations to the desired future states, opportunities to further secure the enterprise in support of HVAs should be considered along with reduced waste and duplication, migration to shared services, closing of performance gaps, and modernization.

(The risk of HVA compromise can be reduced from adjacent systems through proper segmentation, regular security updates and security/privacy controls in place on adjacent systems)

HVA Implementation Standard

HVA.1 – CMS Enterprise and applicable CMS Mission/Business/System architectures must be up to date to reflect the protection needs of the HVA to ensure an adequate level of protection for the HVA extends to the enterprise.

Control Number	Control Name	Priority	CMS Baseline
PM-08	**Critical Infrastructure Plan**	**P1**	**Low** **Moderate** **High**

Control Statement

Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Discussion

Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Implementation Standard

High, Moderate & Low:
Std.1 - The CMS Cybersecurity Integration Center (CCIC) will utilize automated tools to:
1. Develop and publish a Critical Unfractured Plan (CIP), as part of the CMS Continuity of Operations Plan (COOP), that establishes and identifies the criterial for CMS systems that fit the CIP definition defined by NIST as; Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
2. Produce an inventory of organizational systems, to include those operated on behalf of CMS (e.g., by a contractor, vendor, cloud service provider, or other service provider) that have been identified as part of the critical infrastructure .
3. Develop the inventory of organizational systems defined as critical infrastructure and submit the report to DHS CDM per requirements.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
CP-2, CP-4, PE-18, PL-2, PL-1, PM-1, PM-9, PM-11, PM-18, RA-3, SI-12;
	Reference Policy
	DHS: NIPP;
	HSPD: HSPD 7;
	OMB Circular: A-130;
	NIST SP: 800-34, 800-60;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PM-09	**Risk Management Strategy**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

(a) Develop a comprehensive strategy to manage:
1. Security risk to CMS Enterprise and Mission/Business/System operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and
2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;
(b) Implement the risk management strategy consistently across the organization; and
(c) Review and update the risk management strategy at least every three hundred and sixty-five (365) days or as required, to address organizational changes.

Discussion

An organization-wide risk management strategy includes an expression of the security and privacy risk tolerance for the organization; security and privacy risk mitigation strategies; acceptable risk assessment methodologies; a process for evaluating security and privacy risk across the organization with respect to the organization's risk tolerance; and approaches for monitoring risk over time. The senior accountable official for risk management (agency head or designated official) aligns information security management processes with strategic, operational, and budgetary planning processes. The risk executive function, led by the senior accountable official for risk management, can facilitate consistent application of the risk management strategy organization-wide. The risk management strategy can be informed by security and privacy risk-related inputs from other sources, both internal and external to the organization, to ensure the strategy is broad-based and comprehensive.

Privacy risk management processes operate across the life cycle of a system collecting, using, maintaining, and/or disseminating PII. Such privacy risk management processes include, but are not limited to, design requirements, privacy threshold analysis, privacy impact assessments (PIA), and implementation of secure disposition. While Section 208 of the E-Government Act does not require — or prohibit — a PIA for any system, as defined at 40 U.S.C. §11103 (see Section 202(i) of the E-Government Act), CMS and the Mission/Business/System will benefit from conducting a PIA, or similar privacy risk evaluation, as part of the internal risk management process to ensure privacy risks are identified, evaluated, and managed in systems containing PII. For this reason, the ARS extends the requirement to develop a PIA to all systems.

Implementation Standard

High, Moderate & Low:

Std.1 - The CMS Risk Management Office, lead by the Risk Management Executive, will provide leadership and oversight to:
1 - Develop an organization-wide risk management strategy which includes an expression of the security and privacy risk tolerance for the organization; security and privacy risk mitigation strategies; acceptable risk assessment methodologies; a process for evaluating security and privacy risk across the organization with respect to the organization's risk tolerance; and approaches for monitoring risk over time.
2 - The senior accountable official for risk management (agency head or designated official), i.e., Risk Management Executive, aligns information security management processes with strategic, operational, and budgetary planning processes.
3 - The risk executive function, led by the senior accountable official for risk management, i.e., Risk Management Executive, will facilitate consistent application of the risk management strategy organization-wide.
4 - The risk management strategy can be informed by security and privacy risk-related inputs from other sources, both internal and external to the organization, to ensure the strategy is broad-based and comprehensive.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AC-1, AU-1, AT-1, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, 8809 MP-1, PE-1, PL-1, PL-2, PM-2, PM-8, PM-18, PM-28, PM-30, PS-1, PT-1, PT-2, PT-3, RA-1, RA-3, 8810 RA-9, SA-1, SA-4, SC-1, SC-38, SI-1, SI-12, SR-1, SR-2;
	Reference Policy
	Code: 5 U.S.C. §552a, 44 U.S.C. §3506 (a)(3), §3506(g), §3541;
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208;
	HIPAA: 45 C.F.R. §164.308(a)(1)(ii), 45 C.F.R. §164.316(a), 45 C.F.R. §164.530(a)(1)(i), 45 C.F.R. §164.530(c), 45 C.F.R. §164.530(i)(1) - (3);
	NISTIR: 8023;
	NIST SP: 800-30, 800-37r1, 800-39, 800-160, 800-161;
	OMB Circular: A-130 7.g., 8.a.(1), 8.b.(2), and 8.b.(3);
	OMB Memo: M-03-22, M-05-08, M-06-16, M-17-12 Att. 1 B.1 and Att. 2 A.1;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
A comprehensive risk management strategy will include privacy as an input where appropriate to ensure privacy risks to individuals and CMS Businesses/Systems are identified, prioritized, and managed consistently across the business processes, programs, and systems.
In addition to business risks that arise out of privacy violations, such as reputation or liability risks, CMS Enterprise and Mission/Business/System policies should focus on minimizing the risk of harm to individuals.
CMS Enterprise/Business/System privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. While the actual tools used and processes for managing privacy risk will be specific to CMS Business/System missions and resources, conducting a PIA is the first step. The effective PIA will both identify the privacy risks and identify methods that can help mitigate those risks. PIAs will also help to ensure that the Mission/Business programs and systems comply with legal, regulatory, and policy requirements. Finally, PIAs serve as notice to the public regarding privacy practices. (PIAs are performed before developing or procuring systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.)
OMB Memorandum M-03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002, including guidance on the timing for developing PIAs for systems and electronic collections of information.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
High & Moderate:
PRIV.1 - Amend control clause "(a)" to include:
3. Privacy risks to the information (data) including risk to the individual, risk to the system, risk to the CMS Business/System, and risk to the enterprise.

HVA Control Statement

(a) Develop a comprehensive strategy to manage:
1. Security risk to CMS Enterprise and Mission/Business/System operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and
2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;
(b) Implement the risk management strategy consistently across the organization;
(c) Account for HVAs in the development of the enterprise-wide risk management strategy to ensure changes to the enterprise do not create unknown or unacceptable risks to the HVA; and

(c) Review and update the risk management strategy at least every three hundred and sixty-five (365) days or as required, to address organizational changes.
(d) Develop a comprehensive strategy to manage security risks to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems, as well as privacy risks to individuals resulting from the authorized processing of personally identifiable information

HVA Discussion

The enterprise risk management strategy includes a process to evaluate all risks to HVA information and mission critical services. Per OMB M-19-03: "HVA risk assessments should incorporate operational, business, mission, and continuity considerations." Organizations should develop an enterprise wide risk management strategy that includes is holistic and integrated into the three-levels of the organization.
The three-level approach to risk management addresses risk-related concerns at the enterprise level, the mission/business process level, and the HVA system level.

HVA Implementation Standard

At a minimum, organizations should:
(a)Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework,
(b) Establish a risk management strategy for the organization that includes a determination of risk tolerance, identify the missions, business functions, and mission/business processes the HVA system(s) will support
(c) identify HVA stakeholders who have a security interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system
(d) identify assets that require protection
(e) conduct an initial risk assessment of HVA assets and update the risk assessment on an ongoing basis,
(f) define the HVA protection needs and HVA security requirements, and
(g) determine the placement of the HVA within the EA.

Control Number	Control Name	Priority	CMS Baseline
PM-10	**Authorization Process**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

(a) Manage (e.g., document, track, and report) the security and privacy state of CMS Enterprise and Mission/Business/System and the environments in which those systems operate through authorization processes;
(b) Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
(c) Integrate the authorization processes into an organization-wide risk management program.

Discussion

Authorization processes for organizational systems and environments of operation require the implementation of an organization-wide risk management process and associated security and privacy standards and guidelines. Specific roles for risk management processes include a risk executive (function) and designated authorizing officials for each organizational system and common control provider. The organizational authorization processes are integrated with continuous monitoring processes to facilitate ongoing understanding and acceptance of security and privacy risks to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Implementation Standard

High, Moderate & Low:
Std.1 - The CMS Chief Information Security Officer (CISO) will provide leadership and oversight to:
1 - Establish an authorization processes for organizational systems and environments of operation that require the implementation of an organization-wide risk management process and associated security and privacy standards and guidelines.
2 - Establish specific roles for risk management processes following NIST 800-37 Risk Management Framework (RMF) to include a risk management executive (function) and designated attestation officials for each organizational system and common control provider(s) to assist the CMS Authorization Official (AO) in the authorization process.
3 - Establish an Authority-To-Operate workflow as part of the SDLC organizational authorization processes that are integrated with continuous monitoring processes to facilitate ongoing understanding and acceptance of security and privacy risks to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
CA-6, AR-2, AR-7, TR-1, TR-2, CA-7, PL-2;
	Reference Policy
	Code: 5 U.S.C. §552a(e)(10), 44 U.S.C.: §3541;
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208;
	HIPAA: 45 C.F.R. §164.308(a)(2), 45 C.F.R. §164.530(c);
	NIST SP: 800-37, 800-39, 800-115, 800-137;
	OMB Circular: A-130 7.g., 8.a.(1), 8.b.(2), and 8.b.(3);
	OMB Memo: M-03-22, M-05-08, M-10-23, M-14-03, M-16-04, M-19-03, M-20-04;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

The security authorization process provides a means for evaluating whether a system/process has met given privacy safeguards and documentation requirements.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Amend control clause "(a)" to include:

1. Ensure privacy safeguards and privacy documentation requirements, such as privacy impact assessments (PIA) and systems of records notices (SORN) when applicable, have been appropriately addressed prior to issuance of a security authorization within the CMS Enterprise's and Mission/Business/System's security authorization process.
2. The authorization process ensures privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII is included in the assessment decision;

HVA Control Statement

(a) Manage (e.g., document, track, and report) the security and privacy state of CMS Enterprise and Mission/Business/System and the environments in which those HVA systems operate through authorization processes;

(b) Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

(c) Integrate the authorization processes into an organization-wide risk management program.

HVA Discussion

The organization may adopt an enterprise-wide perspective and approach to both the risks posed by the HVA and the related organizational responsibilities as part of the authorization process. The organization should follow a sound, documented and well-understood authorization approach that meets the protection needs of all stakeholders and is recommended for HVAs.

Ongoing authorization (OA) is a time-driven or event-driven authorization process whereby the AO is provided with the necessary and sufficient information regarding the security and privacy state of the HVA to determine whether the mission or business risk of continued HVA operation is acceptable.

HVA Implementation Standard

(a) Implement Information Security Continuous Monitoring (ISCM) program as defined in NIST SP 800-137 per Ongoing Authorization (OA)

(b)Leverage CDM tools and methods to automate collection, review, and alerting requirements of OA where possible

Control Number **PM-11**	**Control Name** **Mission and Business Process Definition**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement

(a) Define a CMS-wide and, if applicable, Mission/Business/System-wide, mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

(b) Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and

(c) Review and revise the mission and business processes at least every three (3) years

Discussion

Protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, systems, and the Nation through the compromise of information (i.e., loss of confidentiality, integrity, availability, or privacy). Information protection and personally identifiable information processing needs are derived from the mission and business needs defined by the stakeholders in organizations, the mission and business processes defined to meet those needs, and the organizational risk management strategy. Information protection and personally identifiable information processing needs determine the required controls for the organization and the systems. Inherent in defining protection and personally identifiable information processing needs, is an understanding of adverse impact that could result if a compromise or breach of information occurs. The categorization process is used to make such potential impact determinations. Privacy risks to individuals can arise from the compromise of personally identifiable information, but they can also arise as unintended consequences or a byproduct of authorized processing of information at any stage of the data life cycle. Privacy risk assessments are used to prioritize the risks that are created for individuals from system processing of personally identifiable information. These risk assessments enable the selection of the required privacy controls for the organization and systems. Mission and business process definitions and the associated protection requirements are documented in accordance with organizational policies and procedures.

Implementation Standard

High, Moderate & Low: Std.1 - The CMS Chief Information Security Officer (CISO) will provide leadership and oversight to: 1 - Establish an security categorization process to meet the FIPS 199 Standards for Security Categorization of Federal Information and Information Systems processes for organizational systems and environments of operation that require the implementation of an organization-wide risk management process and associated security and privacy standards and guidelines.

2 - Establish a process to differentiate between privacy and non-privacy based FISMA systems and be able to baseline privacy activities required; system of record notices (SORNs), privacy threshold analysis (PTA) or fully qualified/approved privacy impact assessments (PIAs), and/or third party website application (TPWA) assessments [when needed] as required for privacy based collection systems.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years

Related Controls	**Reference Policy**

CP-2, PL-2, PM-7, PM-8, RA-2, RA-3, SA-2, AR-2;	Code: 44 U.S.C. §3541;
	Statute: E-Government Act of 2002 (Pub. L. No. 107-347) §208;
	FIPS: 199;
	HIPAA: 45 C.F.R. §164.306(a) and (b), 45 C.F.R. §164.530(c);
	NIST SP: 800-60v1, 800-60v2, 800-160v1;
	OMB Circular: A-130 7.g., 8.b.(1)(b), 8.b.(2)(b), and Appendix IV;
	OMB Memo: M-03-22, M-05-08, M-10-23;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

In addition to business risks that arise out of privacy violations, such as reputation or liability risks, CMS Business/System policies should also focus on minimizing the risk of harm to individuals. Since the effective PIA can be used to help identify the privacy risks to individuals and the PIA is accessible to the public, the PIA will serve as notice to the public regarding the Mission/Business/System privacy practices and processes.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Amend control clause "(b)" to include:

1. Define and implement mission and business processes that include assessment of privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII;

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PM-12	**Insider Threat Program**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

Discussion

Organizations handling classified information are required, under Executive Order 13587 and the National Insider Threat Policy (i.e., ODNI NITP), to establish insider threat programs. The same standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of controlled unclassified and other information in non-national security systems. Insider threat programs include controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior official is designated by the department or agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs require organizations to prepare department or agency insider threat policies and implementation plans; conduct host-based user monitoring of individual employee activities on government-owned classified computers; provide insider threat awareness training to employees; receive access to information from offices in the department or agency for insider threat analysis; and conduct self-assessments of department or agency insider threat posture.

Insider threat programs can leverage the existence of incident handling teams that organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace, including ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues. These precursors can guide organizational officials in more focused, targeted monitoring efforts. However, the use of human resource records could raise significant concerns for privacy. The participation of a legal team, including consultation with the senior agency official for privacy, ensures that monitoring activities are performed in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Implementation Standard

High, Moderate & Low:

Std.1 - As required by the CMS Information System Security and Privacy Policy (IS2P2), the organization implements the insider threat program in accordance with HHS Policy for Monitoring Employee Use of HHS IT Resources. The CIO and CISO will provide leadership and oversight to:

1 - Establish an office of Division of Strategic Information (DSI) in the Information Security and Privacy Group (ISPG) that will take ownership and responsibility for the development of an Insider Threat Program.

2 - Apply standards and guidelines that apply to insider threat programs in classified environments that can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems.

3 - Develop security controls and protocols to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns.

4 - Designate a senior organizational official as Division Director of DSI as the responsible individual to implement and provide oversight for the insider threat program.

5 - The insider threat programs at a minimum, will prepare department/agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis, and conduct self-assessments of department/agency insider threat posture.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years

Related Controls	Reference Policy

AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-1, PM-14, PM-16, PS-3, PS-4, PS-5, PS-7, PS-8, SC-7, SC-38, SI-4;	Code: 5 U.S.C. §552a(e)(5), §552a(e)(5)(9)-(10);
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002; (Pub. L. No. 107-347) §208;
	EO: 13587;
	HHS: Policy for Monitoring Employee Use of HHS IT Resources;
	ODNI: NITP;
	OMB Circular: A-130 7.g.;
	OMB Memo: M-17-12;

	ONDI: National Insider Threat Policy and the Minimum Standards;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

The privacy risks inherent with aggregating sensitive personally identifiable information (PII) from multiple data resources within CMS Businesses/Systems, such as human resource and background investigation information, and the potential for scope creep require the active participation, review, and concurrence of the Privacy Officer.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Amend control to include:

(a) Ensure the insider threat team engages the participation, and obtains concurrence, of the Mission/Business/System's Privacy Officer (or the CMS Senior Official for Privacy when appropriate) prior to implementation within the requirements of the insider threat program.

(b) For existing insider threat programs, conduct an annual review of the program with the Privacy Officer to ensure program meets applicable privacy requirements.

HVA Control Statement

Implement an insider threat program that includes a cross-discipline insider threat incident handling team that accounts for potential impacts to the HVA.

HVA Discussion

Given the sensitivity of the HVA, organizations develop and implement an insider threat program in accordance with ODNI National Insider Threat Task Force's "National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs." A senior official is designated by the department or agency head as the responsible individual to implement and provide oversight for the insider threat program. The program is authorized by policy and outlines the processes executed by the organization to detect and respond to insider threats through technical and non-technical means. Organizations implement controls and capabilities to prevent malicious insider threats actions (e.g., DLP, monitoring, access controls, etc.) and provide insider threat training to all employees and contractors.

HVA Implementation Standard

HVA.1 – Designate a senior CMS official as the responsible individual to implement and provide oversight for the insider threat program.

HVA.2 – Ensure insider threat programs are authorized by policy and outline the processes executed by the organization to detect and respond to insider threats through technical and non-technical means.

HVA.3 – Implement controls and capabilities to prevent malicious insider threat actions (e.g., DLP, monitoring, access controls) and provide insider threat training to all employees and contractors.

Control Number	Control Name	Priority	CMS Baseline
PM-13	**Security and Privacy Workforce**	**P1**	**Low** **Moderate** **High**

Control Statement

Establish a security and privacy workforce development and improvement program.

Discussion

Security and privacy workforce development and improvement programs include defining the knowledge, skills, and abilities needed to perform security and privacy duties and tasks; developing role-based training programs for individuals assigned security and privacy roles and responsibilities; and providing standards and guidelines for measuring and building individual qualifications for incumbents and applicants for security- and privacy-related positions. Such workforce development and improvement programs can also include security and privacy career paths to encourage security and privacy professionals to advance in the field and fill positions with greater responsibility. The programs encourage organizations to fill security- and privacy-related positions with qualified personnel. Security and privacy workforce development and improvement programs are complementary to organizational security and privacy awareness and training programs and focus on developing and institutionalizing the core security and privacy capabilities of personnel needed to protect organizational operations, assets, and individuals.

Implementation Standard

High, Moderate & Low:

Std.1 - As required by the CMS Information System Security and Privacy Policy (IS2P2), the organization implements a security and privacy workforce development and improvement program. The CIO and CISO will provide leadership and oversight to:

1 - Develop Security and privacy workforce development and improvement programs to include defining the knowledge, skills, and abilities needed to perform security and privacy duties and tasks; 2 - Develop role-based training programs for individuals assigned security and privacy roles and responsibilities; 3 - Provide standards and guidelines for measuring and building individual qualifications for incumbents and applicants for security- and privacy-related positions.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AT-2, AT-3;
	Reference Policy
	Code: 5 U.S.C. §552a(e)(9)-(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	EO: 13800 (including National Initiative for Cybersecurity Education [NICE]);
	HHS: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities;
	HIPAA: 45 C.F.R. §164.308(a)(2);
	NIST SP: 800-181;
	OMB Circular: A-130 7.g.;
	OMB Memo: M-17-12;

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): To implement adequate security controls, the CMS Business's/System's security and privacy workforce should be knowledgeable of the applicable privacy and security requirements commensurate with the level of access or responsibility for applying appropriate safeguards. The security workforce should receive role-based training for the privacy requirements commensurate with the level of access or responsibility for applying safeguards to personally identifiable information (PII).	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **PM-14**	**Control Name** **Testing, Training, and Monitoring**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement (a) Implement a process for ensuring that CMS Enterprise and Mission/Business/System plans for conducting security and privacy testing, training, and monitoring activities associated with CMS Enterprise and Mission/Business/System systems: 1. Are developed and maintained; and 2. Continue to be executed; and (b) Review testing, training, and monitoring plans for consistency with the CMS-wide and, if applicable, Mission/Business/System-wide, risk security and privacy management strategy and CMS Enterprise and Mission/Business/System-wide priorities for risk response actions.			
Discussion A process for organization-wide security and privacy testing, training, and monitoring helps ensure that organizations provide oversight for testing, training, and monitoring activities and that those activities are coordinated. With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the three levels of the risk management hierarchy and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing assessments supporting a variety of controls. Security and privacy training activities, while focused on individual systems and specific roles, require coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.			
Implementation Standard High, Moderate & Low: Std.1 - The CIO and CISO will provide leadership and oversight to:			

<table>
<tr><td colspan="2">1 - Develop a process for organization-wide security and privacy testing, training, and monitoring to ensure that CMS provides oversight for testing, training, and monitoring activities and that those activities are coordinated amongst stakeholders following NIST SP 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, and the NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View.
2 - Per NIST SP 800-39, risk management should be addressed at the: Organizational Tier. Business Process Tier. Information Systems Tier.
3 - With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the three levels of the risk management hierarchy and the widespread use of common controls, CMS shall coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing assessments supporting a variety of controls via the CCIC mission and support initiatives.
4 - Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.
Std 2 - The CMS Cybersecurity Integration Center (CCIC) will utilize automated tools to:
1 - Coordinate and consolidate the testing and monitoring activities via the Continuous Diagnostics Monitoring (CDM) and Pen Test programs as prescribed in the CMS INFORMATION SECURITY CONTINUOUS MONITORING (ISCM) STRATEGY AND PROGRAM.
Std 3 - Security and Awareness Training (SAT) Coordinators
1 - Develop a process to track organization-wide security and privacy training activities, while focused on individual systems and specific roles, requiring coordination across all organizational elements.</td></tr>
<tr><td><b>Control Review Frequency</b>
Annually (365 Days)</td><td><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td><b>Related Controls</b>
AT-2, AT-3, CA-7, CP-4, IR-3, PM-12, SI-4;</td><td><b>Reference Policy</b>
Code: 5 U.S.C. §552a(e)(9)-(10);
Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208;
HHS: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities;
NIST SP: 800-16, 800-37, 800-39, 800-53A, 800-115, 800-137;
OMB Circular: A-130 7.g.;
OMB Memo: M-17-12 Att.1, A.2., M-14-03, M-16-04, M-19-03, M-20-04;</td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b>
Discussion for systems processing, storing, or transmitting PII (to include PHI):
It is critical to integrate privacy risk management, compliance monitoring, and testing into the CMS Business/System risk management strategy and the associated testing and training requirements otherwise an important aspect of privacy may be overlooked.</td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="2"><b>HVA Discussion</b></td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>PM-15</b></td><td><b>Control Name</b>
<b>Security and Privacy Groups and Associations</b></td><td><b>Priority</b>
<b>P3</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Establish and institutionalize contact with selected groups and associations within the security and privacy communities:
(a) To facilitate ongoing security and privacy education and training for CMS and Mission/Business/System personnel;
(b) To maintain currency with recommended security and privacy practices, techniques, and technologies; and
(c) To share current security and privacy information, including threats, vulnerabilities, and incidents.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Ongoing contact with security and privacy groups and associations is important in an environment of rapidly changing technologies and threats. Groups and associations include special interest groups, professional associations, forums, news groups, users' groups, and peer groups of security and privacy professionals in similar organizations. Organizations select security and privacy groups and associations based on missions and business functions. Organizations share threat, vulnerability, and incident information as well as contextual insights, compliance techniques, and privacy problems consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.</td></tr>
</table>

To maximize CMS's ability to maintain compliance with privacy requirements and privacy best practices, CMS must ensure its privacy professionals, especially at the enterprise level, actively engage with both its security community and external communities, such as the Federal privacy community, to remain current and to share lessons-learned or other privacy-related information.

Implementation Standard

High, Moderate & Low:

Std.1 - The CIO and CISO will provide leadership and oversight to:

1 - Develop a process for promoting ongoing contact with security and privacy groups, and professional information cybersecurity associations to support security awareness amongst stakeholders to promote an environment of rapidly changing technologies and threats.

2 - Groups and associations can include; special interest groups, professional associations, forums, news groups, users' groups, and peer groups of security and privacy professionals.

3 - Organizations select security and privacy groups and associations based on missions and business functions.

4 - Organizations share threat, vulnerability, and incident information as well as contextual insights, compliance techniques, and privacy problems consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines..

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
SA-11, SI-5;
	Reference Policy
	Code: 5 U.S.C. §552a, 44 U.S.C. §3506 (a)(3), §3506(g), §3541;
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208;
	HIPAA: 45 C.F.R. §164.530(a)(1)(i), 45 C.F.R. §164.530(i)(1) - (3);
	NIST SP: 800-37, 800-39, 800-137;
	OMB Circular: A-130 7.g.;
	OMB Memo: M-03-22, M-05-08, M-14-03, M-16-04, M-17-12, M-19-03, M-20-04;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Ongoing contact with privacy groups and associations is of paramount importance to both the CMS Enterprise and to the Mission/Business/System in an environment of rapidly changing technologies and threats. Privacy groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of privacy professionals in similar organizations. CMS and CMS Businesses/Systems select groups and associations based on CMS and CMS Business/System missions/business functions. CMS and CMS Businesses/Systems share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PM-16	**Threat Awareness Program**	**P1**	**Low** **Moderate** **High**

Control Statement

Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

Discussion

Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it may be more likely that adversaries can successfully breach or compromise organizational systems. One of the best techniques to address this concern is for organizations to share threat information including threat events (i.e., tactics, techniques, and procedures) that organizations have experienced; mitigations that organizations have found are effective against certain types of threats; and threat intelligence (i.e., indications and warnings about threats). Threat information sharing may be bilateral or multilateral. Bilateral threat sharing includes government-to-commercial and government-to-government cooperatives. Multilateral threat sharing includes organizations taking part in threat-sharing consortia. Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.

Implementation Standard High, Moderate & Low: Std.1 - The CIO and CISO will provide leadership and oversight to mitigate the APT landscape: 1 - Constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it may be more likely that adversaries can successfully breach or compromise organizational systems. One of the best techniques to address this concern is for organizations to share threat information including threat events (i.e., tactics, techniques, and procedures) that organizations have experienced; mitigations that organizations have found are effective against certain types of threats; and threat intelligence (i.e., indications and warnings about threats). 2 - Threat information sharing may be bilateral or multilateral. Bilateral threat sharing includes government-to-commercial and government-to-government cooperatives. Multilateral threat sharing includes organizations taking part in threat-sharing consortia. Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared. 3 - Develop a Threat Awareness program to address the APT landscape within the CCIC - Cyber Threat Intelligence and Division of Strategic Information (DSI) - Threat Intelligence (?TBD?) to share APT information to reduce the risk profile and landscape at CMS.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls IR-4, IR-10, PM-12;	**Reference Policy** Statute: Cybersecurity Enhancement Act of 2014;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PM-16(01)	**Automated Means for Sharing Threat Intelligence**		**Low** **Moderate** **High**

Control Statement Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.	
Discussion To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By using well-established frameworks, services, and automated tools, organizations improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.	
Implementation Standard High, Moderate & Low: Std.1 - The CCIC Cyber Threat Intelligence section will: 1 - Automate monitoring capabilities for cyber threat intelligence information from threat observables and indicators via sensor mechanisms. 2 - Utilize well-established frameworks, services, and automated tools, so CMS may improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls None;	**Reference Policy** See Control PM-16;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**

<table>
<tr><td><b>PM-17</b></td><td><b>Protecting Controlled Unclassified Information on External Systems</b></td><td><b>P1</b></td><td><b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
(a) Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards.
(b) Review and update the policy and procedures every three (3) years</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Controlled unclassified information is defined by the National Archives and Records Administration along with the safeguarding and dissemination requirements for such information and is codified in the Code of Federal Regulations, Title 32, Controlled Unclassified Information and specifically, for systems external to the federal organization, in 32 CFR 2002.14h. The policy prescribes the specific use and conditions to be implemented in accordance with organizational procedures, including via its contracting processes.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High, Moderate & Low:
Std.1 - The CIO and CISO will provide leadership and oversight to:
1 - Work in conjunction with the CUI program office to identify and post CUI designations to all appropriate documents published [externally?].</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
CA-6, PM-10;</td><td colspan="2"><b>Reference Policy</b>
Code: 32 C.F.R 2002;
NARA: CUI;
NIST: SP 800-171;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
PM-18</td><td><b>Control Name</b>
Privacy Program Plan</td><td><b>Priority</b>
P1</td><td><b>CMS Baseline</b>
Low
Moderate
High</td></tr>
<tr><td colspan="4"><b>Control Statement</b>
(a) Develop and disseminate a CMS Enterprise-wide, with supporting Mission/Business/System-wide (when needed) privacy program plan that provides an overview of CMS's privacy program, and:
1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;
2. Provide an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;
3. Include the role of the Senior Official for Privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;
4. Describe management commitment, compliance, and the strategic goals and objectives of the privacy program;
5. Reflect coordination among CMS entities responsible for the different aspects of privacy; and
6. Is approved by a senior CMS official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and
(b) Update the CMS Enterprise-wide, with supporting Mission/Business/System-wide (when needed) privacy program plan as needed to address changes in federal privacy laws, policy, organizational changes, and problems identified during plan implementation or privacy control assessments, but no less often than every two years.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
A privacy program plan is a formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program; the resources dedicated to the privacy program; the role of the senior agency official for privacy and other privacy officials and staff; the strategic goals and objectives of the privacy</td></tr>
</table>

program; and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. Privacy program plans can be represented in single documents or compilations of documents.

The CMS Senior Official for Privacy is responsible for selecting the privacy controls CMS and identifying which controls will be treated as program management, common, system-specific, and/or hybrid. Privacy program plans provide sufficient information about the privacy program management and common controls (including the specification of parameters and assignment and selection statements explicitly or by reference) to enable control implementations that are unambiguously compliant with the intent of the plans and a determination of the risk incurred if the plans are implemented as intended.

(i) Program management controls are generally implemented Enterprise level and are essential for managing CMS's privacy program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular system. The privacy plans for individual systems and the organization-wide privacy program plan together, provide complete coverage for the privacy controls employed within the organization.

(ii) Common controls are documented within the Enterprise privacy program plan unless the controls have already been included in either the Information Security Program Plan (PM-1) or, when identified as system-specific, a separate privacy plan specific to the Mission/System/Business. The CMS Enterprise-wide privacy program plan indicates when separate privacy plans will need to contain descriptions of the selected privacy controls.

Effective implementation of privacy and security controls requires a collaborative partnering of the Senior Official for Privacy, CIO, and CISO. To maximize CMS's ability to comply with changing privacy requirements and best practices, CMS must monitor federal privacy laws and policy for changes that affect the privacy program. Working with other groups (PM-15), also helps in this effort.

Privacy risk management processes operate across the life cycle of a system collecting, using, maintaining, and/or disseminating PII. Such privacy risk management processes include, but are not limited to, design requirements, privacy threshold analysis, privacy impact assessments (PIA), and implementation of secure disposition. While Section 208 of the E-Government Act does not require — or prohibit — a PIA for any system, as defined at 40 U.S.C. §11103 (see Section 202(i) of the E-Government Act), CMS and the Mission/Business/System will benefit from conducting a PIA, or similar privacy risk evaluation, as part of the internal risk management process to ensure privacy risks are identified, evaluated, and managed in systems containing PII. For this reason, the ARS extends the requirement to develop a PIA to all systems.

The CMS Senior Official for Privacy develops privacy program plans to document the privacy requirements CMS must meet and the privacy and security controls in place or planned for meeting those requirements. The privacy program plan serves as evidence of CMS's privacy operations and supports resource requests by the SOP. In addition to selecting the privacy-related controls, the CMS Enterprise-level Privacy Program Plan, should include:

(i) Processes for conducting privacy risk assessments;
(ii) Templates and guidance for completing Privacy Impact Assessments (PIA and System of Records Notices (SORN);
(iii) Privacy training and awareness requirements;
(iv) Requirements for contractors processing PII;
(v) Plans for eliminating unnecessary PII holdings; and
(vi) A framework for measuring annual performance goals and objectives for implementing identified privacy controls

Note: CMS includes protecting PII within the information security program plan. This includes the definition of roles and responsibilities associated with protecting PII.

Implementation Standard

High & Moderate:

Std.1 - Development of the strategic CMS privacy plan must be done in consultation with the CMS Chief Information Officer (CIO) and CMS Chief Information Security Officer (CISO).

The organization establishes and institutionalizes contact for its privacy professionals with selected groups and associations within the privacy community:

(a) To facilitate ongoing privacy education and training for organizational personnel;
(b) To maintain currency with recommended privacy practices, techniques, and technologies; and
(c) To share current privacy-related information including threats, vulnerabilities, and incidents.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

PM-8, PM-9, PM-15, PM-19, AR-1	Code: 5 U.S.C. §552a, 44 U.S.C. §3541, §3506(a)(3), §3506(g);
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208;
	HIPAA: 45 C.F.R. §164.530(a)(1)(i), 45 C.F.R. §164.530(c), 45 C.F.R. §164.530(i)(1) - (3);
	OMB Circular: A-130 7.g., 8.a.(1), AE3798.b.(2), and 8.b.(3);
	OMB Memo: M-03-22, M-05-08, M-10-23, M-17-12;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI): The development and implementation of a comprehensive governance and privacy program demonstrates CMS and CMS Business/System accountability for and commitment to the protection of individual privacy. The CMS Enterprise-level Privacy Plan may be supplemented by Mission/Business/System specific Privacy Plans that are customized for CMS and CMS Business/System structures, requirements, and resources. Such plans may vary in comprehensiveness. For example, a one-page privacy plan may augment the CMS Enterprise Privacy Plan and cover privacy policies, documentation, and controls already in place, such as Privacy Impact Assessments (PIA) and System of Records Notices (SORN). A more comprehensive plan could include a baseline of privacy controls selected from this appendix and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls.
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PM-19	**Privacy Program Leadership Role**	**P1**	**Low** **Moderate** **High**

Control Statement Appoint a Senior Official for Privacy (CIO, CISO defined in the roles and responsibilities section of the IS2P2) with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the CMS Enterprise-wide privacy program.
Discussion The privacy officer is an organizational official. For federal agencies, as defined by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, this official is designated as the senior agency official for privacy. Organizations may also refer to this official as the chief privacy officer. The senior agency official for privacy also has a role in the data management board (see PM-23) and the data integrity board (see PM-24).
Implementation Standard High, Moderate & Low: Std.1 - Appoint a Senior Official for Privacy (CIO, CISO defined in the roles and responsibilities section of the IS2P2) with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the CMS Enterprise-wide privacy program.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

PM-18, PM-20, PM-23, PM-24;	Code: 5 U.S.C. §552a, 44 U.S.C. §3506(a)(3), §3506(g), §3541;
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208;
	HIPAA: 45 C.F.R. §164.530(a)(1)(i), 45 C.F.R. §164.530(i)(1) - (3);
	OMB Circular: A-130;
	OMB Memo: M-03-22, M-05-08, M-17-12;

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): Accountability begins with the appointment of a SOP with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SOP, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development, implementation, and enforcement of privacy policies and procedures;

(ii) defines roles and responsibilities for protecting PII;
(iii) determines the level of information sensitivity with regard to PII holdings;
(iv) identifies the laws, regulations, and internal policies that apply to the PII;
(v) monitors privacy best practices; and
(vi) monitors/audits compliance with identified privacy controls.

To further accountability, the SOP develops privacy plans to document the privacy requirements within CMS and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of CMS and CMS Business/System privacy operations and supports resource requests by the SOP.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PM-20	**Dissemination of Privacy Program Information**	**P1**	**Low** **Moderate** **High**

Control Statement

Maintain a central resource webpage on CMS’s principal public website (provided by HHS) that serves as a central source of information about CMS’s privacy program and work with HHS to:
(a) Ensure that the public has access to information about CMS's privacy activities and can communicate with CMS's Senior Official for Privacy;
(b) Ensure that CMS privacy practices and reports are publicly available; and
(c) Employ publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to CMS's privacy offices regarding privacy practices.

Discussion

For federal agencies, the webpage is located at www.[agency].gov/privacy. Federal agencies include public privacy impact assessments, system of records notices, computer matching notices and agreements, [PRIVACT] exemption and implementation rules, privacy reports, privacy policies, instructions for individuals making an access or amendment request, email addresses for questions/complaints, blogs, and periodic publications.

Implementation Standard

High, Moderate & Low:

Std.1 - Implement and maintain a central resource webpage on CMS’s principal public website (https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy) that serves as the central source of information about CMS’s privacy program to:
(a) Publicly access information about CMS's privacy activities and provide a communication channel with the CMS's Senior Official for Privacy via the Privacy@cms.hhs.gov email address;
(b) Post CMS privacy practices and any publicly consumable reports to the public website; SORNs, PIAs, PTAs, TPWAs, DUAs, etc.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years

Related Controls	Reference Policy

AC-3, PM-19, PT-5, PT-7, RA-8	Statute: Privacy Act (P.L. 93-579), December 1974;
	OMB Circular: A-130;
	OMB Memo: M-19-03;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Making information about the CMS (and CMS Business/System's) privacy program readily available to the public reduces the burden on individuals wanting to better understand the CMS and CMS Business/System privacy practices; and reduces burden on privacy offices and program officials by providing answers to common privacy questions through an easily accessible forum.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PM-20(01)	**Privacy Policies on Websites, Applications, and Digital Services**		**Low** **Moderate** **High**

Control Statement

Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:
(a) Are written in plain language and organized in a way that is easy to understand and navigate;
(b) Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and
(c) Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

Discussion

Organizations post privacy policies on all external-facing websites, mobile applications, and other digital services. Organizations post a link to the relevant privacy policy on any known, major entry points to the website, application, or digital service. In addition, organizations provide a link to the privacy policy on any webpage that collects personally identifiable information. Organizations may be subject to applicable laws, executive orders, directives, regulations, or policies that require the provision of specific information to the public. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Implementation Standard

Std.1 - Appoint a CMS Chief Information Security Officer (CISO) who supports the CMS Authorization Official (AO) with the mission and resources necessary to coordinate, develop, implement, and maintain the CMS enterprise-wide information security and privacy program.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**
None;	[PRIVACT], [OMB A-130], [OMB M-17-06]

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PM-21	Accounting of Disclosures	P1	Low Moderate High

Control Statement

a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:
1. Date, nature, and purpose of each disclosure; and
2. Name and address, or other contact information of the person or organization to which the disclosure was made;

b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and
c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

Discussion

The purpose of accounting of disclosures is to allow individuals to learn to whom their personally identifiable information has been disclosed; to provide a basis for subsequently advising recipients of any corrected or disputed personally identifiable information; and to provide an audit trail for subsequent reviews of organizational compliance with conditions for disclosures. For federal agencies, keeping an accounting of disclosures is required by the [PRIVACT]; agencies should consult with their senior agency official for privacy and legal counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision.

Organizations can use any system for keeping notations of disclosures, if it can construct from such a system, a document listing of all disclosures along with the required information. Automated mechanisms can be used by organizations to determine when personally identifiable information is disclosed, including commercial services providing notifications and alerts. Accounting of disclosures may also be used to help organizations verify compliance with applicable privacy statutes and policies governing disclosure or dissemination of information and dissemination restrictions.

Implementation Standard

Std. 1 - Provide individuals the right to an accounting of disclosures of their Personally Identifiable Information (PII) and Protected Health Information (PHI) by CMS or its business associates.

1 - Develop a system to identify and track notations of disclosures by listing all disclosures along with the required information.

2 - At a minimum, collect the following information

a. Date, nature, and purpose of each disclosure; and b. Name and address, or other contact information of the person or organization to which the disclosure was made;

b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and

c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

Std. 2 Account for disclosures as required under the Privacy Act, HIPAA, and HITECH.

Std. 3 -Develop specific process for accounting of disclosures.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

AU-2, PM-23, SI-18, PT-2	Code: 5 U.S.C. §552a(c), §552a(c)(1), §552a(c)(3), §552a(j), §552a(k);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	HIPAA: 45 C.F.R. §164.528;
	OMB Circular: A-130;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

While both the Privacy Act and HIPAA require accountings of disclosures in certain circumstances, there are differences in the requirements to account for disclosures under the Privacy Act and under HIPAA.

The CMS Senior Official for Privacy periodically consults with CMS Business Owners and System Owners for Mission-related/Business-related systems of records to ensure the required accountings of disclosures are being properly maintained and provided to persons named in those records (i.e., ensure consistency with the dictates of the Privacy Act). Systems are required to keep an accounting of disclosures when the disclosures are made to individuals with a documented need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.S.C. §552a(c)(3). The CMS Administrator may also promulgate rules to exempt certain systems of records from the requirement to provide the accounting of disclosures to individuals.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PM-22	**Personally Identifiable Information Quality Management**	**P1**	**Low** **Moderate** **High**

Control Statement

Develop and document organization-wide policies and procedures for:

(a) Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;

(b) Correcting or deleting inaccurate or outdated personally identifiable information;

(c) Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities, and

(d) Appeals of adverse decisions on correction or deletion requests.

Discussion

Personally identifiable information quality management include steps that organizations take to confirm the accuracy and relevance of personally identifiable information throughout the information life cycle. The information life cycle includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition of personally identifiable information. Organizational policies and procedures for personally identifiable information quality management are important because inaccurate or outdated personally identifiable information maintained by organizations may cause problems for individuals. Organizations consider the quality of personally identifiable information involved in business functions where inaccurate information may result in adverse decisions or the denial of benefits and services, or the disclosure of the information may cause stigmatization. Correct information, in certain circumstances, can cause problems for individuals that outweigh the benefits of organizations maintaining the information. Organizations consider creating policies and procedures for the removal of such information.

The senior agency official for privacy ensures that practical means and mechanisms exist and are accessible for individuals or their authorized representatives to seek the correction or deletion of personally identifiable information. Processes for correcting or deleting data are clearly defined and publicly available. Organizations use discretion in determining whether data is to be deleted or corrected based on the scope of requests, the changes sought, and the impact of the changes. Additionally, processes include the provision of responses to individuals of decisions to deny requests for correction or deletion. The responses include the reasons for the decisions, a means to record individual objections to the decisions, and a means of requesting reviews of the initial determinations.

Organizations notify individuals or their designated representatives when their personally identifiable information is corrected or deleted to provide transparency and confirm the completed action. Due to complexity of data flows and storage, other entities may need to be informed of correction or deletion. Notice supports the consistent correction and deletion of personally identifiable information across the data ecosystem.

When a record is used to make determinations related to a right, benefit, or privilege for an individual, the Privacy Act of 1974, as amended, requires the information used be accurate, relevant, timely, and complete to assure fairness to the individual in the determination. As such, CMS must take measures to ensure the quality of all its PII, even if it is not protected directly by the Privacy Act. CMS's data quality assurance process should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office. As such, when PII is of a sufficiently sensitive nature (e.g., a patient's health data), CMS Businesses/Systems incorporate mechanisms into systems, and develop corresponding processes and procedures, for how frequently, and by what method, the PII is to be validated and updated (re-validated). Frequency of confirmation should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the CMS Business/System owner in consultation with the CMS privacy office.

● Validating PII is used to ensure information used in the determination of an individual's rights, benefits, or privileges is based on accurate, timely, and relevant information.

● Re-validation of PII is used to ensure information used in the determination of an individual's rights, benefits, or privileges continues to be based on accurate, timely, and relevant information.

Implementation Standard

High & Moderate:

Std 1 - Provide individuals the right to redress of their Personally Identifiable Information (PII) and Protected Health Information (PHI) by CMS or its business associates for systems that:

1 - Collects PII directly from the individual to the greatest extent practicable;

2 - Checks for, and corrects as necessary, inaccurate or outdated PII no less often than once every 365 days or as directed by the Data Integrity Board

3 - Does not collect PII from the individual or individual's authorized representative, request the revalidation of the accuracy of the collected PII no less often than once every 365 days or as directed by the Data Integrity Board.

4 - Issues publicly available guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Std 2 - Revalidation must occur as frequently as is necessary to ensure the PII is accurate, relevant, timely, and complete; commensurate with the impact of the determination to an individual's rights, benefits, or privileges as determined by the Mission/Business/System owner and CMS Senior Official for Privacy.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
PM-23, SI-18;
	Reference Policy
	Code: 5 U.S.C. §552a(a)(8)(A), §552a(c), §552a(e), §552a(e)(5), §552a(o), §552a(p), §552a(u), 44 U.S.C. §3501;
	Statute: Privacy Act of 1974 (P.L. 93-579), Paperwork Reduction Act, Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554) App C §515 and 114 Stat. 2763A-153-4;
	NIST SP: 800-188;
	OMB Circular: A-130 Appendix I, 7.g., and 8.a.9;

	OMB Memo: M-17-12;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

When a record is used to make determinations related to a right, benefit, or privilege for an individual, the Privacy Act of 1974, as amended, requires the information used be accurate, relevant, timely, and complete to assure fairness to the individual in the determination. CMS needs to ensure the quality of all of its PII, even if the PII is not protected by the Privacy Act. CMS's data quality assurance process needs to be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the Mission/Business/System owner in consultation with the CMS Senior Official for Privacy.

CMS Systems need to take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into systems using automated address verification look-up application programming interfaces (API). The measures a CMS Mission/Business/System owner takes to protect data quality need to be based on the nature and context of the PII, how the PII is to be used, and how it was obtained. (Measures taken to validate the accuracy of PII used to make determinations about the rights, benefits, or privileges of individuals under federal programs may need to be more comprehensive than those used to validate less sensitive PII.) Additional steps may be necessary to validate PII obtained from sources other than the individuals or authorized representatives of the individuals.

● When PII is of a sufficiently sensitive nature (e.g., a patient's health data), CMS Mission/Business/System owners need to incorporate data quality and validation mechanisms into systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated and validated. Validating PII used to determine a right, benefit, or privilege for an individual ensures the determination is based on accurate, timely, and relevant information. Procedures for validating PII need to be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

● When PII is of a sufficiently sensitive nature (such as, but not limited to, when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit or adjudication of an employee's clearance), CMS Mission/Business/System owners need incorporate data quality and validation mechanisms into systems and develop corresponding procedures for how frequently, and by what method, the information is to be confirmed (validated as) accurate, relevant, timely, and complete. Frequency of confirmation should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

In addition to the initial validation of the information, revalidation of PII used to determine a right, benefit, or privilege for an individual is necessary to ensure the determination is based on the most accurate, timely, and relevant information. Frequency of revalidation should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Amend control to include:

(e) Collects PII directly from the individual to the greatest extent practicable;

(f) Checks for, and corrects as necessary, inaccurate or outdated PII no less often than once every 365 days or as directed by the Data Integrity Board. Where PII is not collected from the individual or individual's authorized representative, request the revalidation of the accuracy of the collected PII no less often than once every 365 days or as directed by the Data Integrity Board.

(g) Issues publicly available guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

PRIV.2 - Revalidation must occur as frequently as is necessary to ensure the PII is accurate, relevant, timely, and complete; commensurate with the impact of the determination to an individual's rights, benefits, or privileges as determined by the Mission/Business/System owner and CMS Senior Official for Privacy.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PM-23	**Data Governance Body**	**P1**	**Low** **Moderate** **High**

Control Statement

Establish a Data Governance Body consisting of CMS-defined roles (defined in the CMS IS2P2 Roles and Responsibilities) with CMS -defined responsibilities (defined in the IS2P2).

Discussion

A Data Governance Body can help ensure that the organization has coherent policies and the ability to balance the utility of data with security and privacy requirements. The Data Governance Body establishes policies, procedures, and standards that facilitate data governance so that data, including personally identifiable information, is effectively managed and maintained in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidance. Responsibilities can include developing and implementing guidelines supporting data modeling, quality, integrity, and de-identification needs of personally identifiable information across the information life cycle and reviewing and approving applications to release data outside of the organization, archiving the applications and the released data, and performing post-release monitoring to ensure that the assumptions made as part of the data release continue to be valid. Members include the chief information officer, senior agency information security officer, and senior agency official for privacy. Federal agencies are required to establish a Data Governance Body with specific roles and responsibilities in accordance with the Foundations for Evidence-Based Policymaking Act of 2018 and policies set forth under OMB M-19-23.

The CMS Data Integrity Board supports the CMS Data Governance Body by ensuring data integrity-related processes and procedures are properly documented and maintained. This information can then be used by the CMS Data Governance Body to policies, procedures, and standards that facilitate data governance are effective.

Implementation Standard

High, Moderate & Low:

Std.1 - The CIO, CISO, and Senior Official for Privacy (SOP) will provide leadership and oversight to: 1 - Charter and implement a CMS Data Governance Body by ensuring data integrity-related processes and procedures are properly documented and maintained.

2 - This information can then be used by the CMS Data Governance Body to develop policies, procedures, and standards that facilitate the data governance in order to ensure the governance is effective.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years

Related Controls	**Reference Policy**

AT-2, AT-3, PM-19, PM-22, PM-24, PT-8, SI-4, SI-19;	Code: 5 U.S.C. §552a, §552a(a)(8), §552a(o), §552a(p), §552a(u), 44 U.S.C. §3541, §3506(a)(3), §3506(g);
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208, Foundations for Evidence-Based Policymaking Act of 2018 (P.L. 115-435);
	HIPAA: 45 C.F.R. §164.530(a)(1)(i), 45 C.F.R. §164.530(i)(1) - (3);
	NIST SP: 800-188;
	OMB Circular: A-130;
	OMB Memo: M-03-22, M-05-08, M-17-12, M-19-23;

Privacy Discussion

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Amend control to include:

(a) Oversee processes to ensure the integrity of personally identifiable information (PII) through existing security and privacy controls.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PM-24	**Data Integrity Board**	**P1**	**Low** **Moderate** **High**

Control Statement

Establish a Data Integrity Board to:

(a) Review proposals to conduct or participate in a matching program;

(b) Conduct an annual review of all matching programs in which CMS has participated.

Discussion

A Data Integrity Board is the board of senior officials designated by the head of a federal agency that is responsible for, among other things, reviewing the agency's proposals to conduct or participate in a matching program and conducting an annual review of all matching programs in which the agency has participated. As a general matter, a matching program is a computerized comparison of records from two or more automated systems of records (required by the Privacy Act of 1974), or an automated system of records and automated records maintained by a non-Federal agency (or agent thereof). A matching program either pertains to Federal benefit programs or Federal personnel or payroll records. At a minimum, the Data Integrity Board includes the Inspector General of the agency, if any, and the senior agency official for privacy.

CMS entities conducting or participating in CMAs with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. CMS's Data Integrity Board coordinates with the HHS Data Integrity Board.

The Data Integrity Board will ensure that controls are in place to maintain both the quality and the integrity of data shared under sharing agreements such as a Computer Matching Agreement (CMA). Additionally, the CMS Data Integrity Board is required to coordinate with the HHS Data Integrity Board.

To support CMS's data quality assurance processes, as required under the Privacy Act, the Data Integrity Board oversees the validation process used to ensure inaccurate or outdated PII is properly addressed (e.g., redacted, revalidated).

Implementation Standard

High, Moderate & Low:

Std.1 - The CIO, CISO, and Senior Official for Privacy (SOP) will provide leadership and oversight to: 1 - Charter and implement a CMS Data Integrity Board that supports the CMS Data Governance Body by ensuring data integrity-related processes and procedures are properly documented and maintained.

2 - The Data Integrity Board will ensure that controls are in place to maintain both the quality and the integrity of data shared under sharing agreements such as a Computer Matching Agreement (CMA). Additionally, the CMS Data Integrity Board is required to coordinate with the HHS Data Integrity Board.

3 - To support CMS's data quality assurance processes, as required under the Privacy Act, the Data Integrity Board oversees the validation process used to ensure inaccurate or outdated PII is properly addressed (e.g., redacted, revalidated).

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
AC-4, PM-19, PM-22, PM-23, PM-33, PT-8;
	Reference Policy
	Code: 5 U.S.C. §552a(a)(8), §552a(a)(8)(A), §552a(o), §552a(p), §552a(u);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	OMB Circular: A-108, A-130 Appendix I and Appendix II;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under CMAs.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Amend control to include:

(a) Ensure CMS's Computer Matching Agreements (CMA) comply with the computer matching provisions of the Privacy Act.

(b) Ensure published guidelines ensure quality, utility, objectivity, and integrity of disseminated information.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PM-25	**Minimization of PII Used in Testing, Training, and Research**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;

(b) Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;

(c) Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and

(d) Review and update policies and procedures with a defined frequency (defined in applicable System security and privacy plans) that does not to exceed three hundred sixty-five (365) days.

Discussion

The use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Organizations consult with the senior agency official for privacy and/or legal counsel to ensure that the use of personally identifiable information in testing, training, and research is compatible with the original purpose for which it was collected. When possible, organizations use placeholder data to avoid exposure of personally identifiable information when conducting testing, training, and research.

Implementation Standard

High, Moderate & Low:

Std.1 - The use of personally identifiable information in testing, research, and training, commonly referred to as "lower operating environments", is not permitted due to the fact
that the lower environments are not authorized for PII/PHI production level data by the CMS Authorization Official (AO). The IS2P2 will reflect the new policy concerning
restricting the use of PII/PHI in owner environments. 1 - PII/PHI Data used for testing, research, and training in lower environments must
be redacted or masked to ensure no PII/PHI production or "live" data are not used in the lower environments which would constitute an unauthorized disclosure of PII/PHI and
create a potential incident response and breach response for PII. 2 -
Anonymizing PII is one technique to reduce risk and decrease the potential impact if the PII is compromised. CMS and CMS Businesses/Systems must minimize risk to privacy
of PII by using techniques such as de-identification. 3 - For systems that must use "live" or production PII/PHI data based on an
authorized mission or business case that is in alignment with the original purpose for which it was collected as prescribed in the System of Records Notice(s) (SORN[s]), the
system must have the lower environments authorized by the CMS AO following the ATO process like any other production system. 4 -
If the system cannot meet the anonymizing or authorization requirements for the lower environments, then the system must request a Risk Based Decision (RBD) for risk
acceptance from the AO until the lower environments can be brought into compliance with the requirement as prescribed in option 1 or 2.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls PM-23, PT-3, SA-3, SA-8, SI-12	**Reference Policy** OMB Circular: A-130 Appendix II;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

When developing and testing systems, PII is at a heightened risk for accidental loss, theft, or compromise. Therefore, the organization needs to take measures to reduce that risk. Anonymizing PII is one technique to reduce risk and decreases the potential impact if the PII is compromised. CMS and CMS Businesses/Systems can minimize risk to privacy of PII by using techniques such as de-identification.

CMS and CMS Businesses/Systems often use PII for testing new applications or systems prior to deployment. CMS and CMS Businesses/Systems also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, CMS and CMS Businesses/Systems must take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. CMS and CMS Businesses/Systems must consult with the Senior Official for Privacy (SOP) and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected.

When PII is of a sufficiently sensitive nature, to the maximum extent possible, PII should be anonymized in accordance with NIST SP 800-122 prior to its use in development or testing.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Amend control to include:

(e) Conduct an initial evaluation of PII holdings needed for internal testing, training, and research and establish and follow a schedule for regularly reviewing those holdings, no less often than once every three hundred sixty-five (365) days, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

(f) Instrument the internal testing, training, and research environments to comply with the CMS minimal baselines for systems storing, processing, or transmitting PII (to include PHI).

(g) Where feasible, use techniques to minimize the risk to privacy of using PII for research, testing, or training.

HVA Control Statement

HVA Discussion

Control Number	Control Name	Priority	CMS Baseline
PM-26	**Complaint Management**	**P1**	**Low** **Moderate** **High**

Control Statement

Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the CMS Mission/Business/System privacy practices that includes:

(a) Mechanisms that are easy to use and readily accessible by the public;

(b) All information necessary for successfully filing complaints;

(c) Tracking mechanisms to ensure all complaints received are reviewed and addressed within CMS-defined time period [ODP = within 24 hours from timestamp of submission]

(d) Acknowledgement of receipt of complaints, concerns, or questions from individuals within CMS-defined time period [ODP = within 24 hours from timestamp of submission] and

(e) Response to complaints, concerns, or questions from individuals within CMS-defined time period [ODP = within 72 hours from timestamp of submission]

Discussion

Complaints, concerns, and questions from individuals can serve as a valuable source of input to organizations that ultimately improves operational models, uses of technology, data collection practices, and controls. Mechanisms that can be used by the public include telephone hotline, email, or web-based forms. The information necessary for successfully filing complaints includes contact information for the senior agency official for privacy or other official designated to receive complaints. Privacy complaints may also include personally identifiable information.

(f) Checks for, and corrects as necessary, inaccurate or outdated PII no less often than once every 365 days or as directed by the Data Integrity Board. Where PII is not collected from the individual or individual's authorized representative, request the revalidation of the accuracy of the collected PII no less often than once every 365 days or as directed by the Data Integrity Board.

Implementation Standard

High, Moderate & Low:

Std.1 - The Senior Official for Privacy (SOP) where PII/PHI is collected for a system will

1 - Establish a complaint management process that ensures complaints are addressed via the Privacy@cms.hhs.gov email as the primary point of enter for individuals who participate in government activities that may impact privacy as an avenue for redress.

2 - Establish tracking mechanisms to ensure all complaints received are reviewed and addressed within 24 hours of receipt from timestamp of the submission from the requestor.

3 - Issue an acknowledgement of receipt of complaints, concerns, or questions from individuals within 24 hours from timestamp of receipt of the submission from the requestor.

4 - Respond initially to complaints, concerns, or questions from individuals within 72 hours from timestamp of receipt of the submission from the requestor.

5 - If the initial analysis/response requires more than 72 hours to address the original complaints, concerns, or questions due to the complexity of the inquiry, then provide an estimate to the individual of the time when a response can be generated, and keep the requestor informed at an agreed to time interval for updates within 72 hours from timestamp of receipt of the submission from the requestor.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years

Related Controls	Reference Policy

IR-7, IR-9, PM-22, SI-18;	Code: 5 U.S.C. §552a;
	HIPAA: 45 C.F.R. §164.520(b)(1)(vi), 45 C.F.R. §164.530 (d);
	OMB Circular: A-130;
	OMB Memo: M-17-12, M-08-09;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Establishing a complaint management process ensures complaints are addressed in a timely manner and provides an avenue for individuals to participate in government activities that may impact privacy. Information received from complaints provides external input regarding CMS and CMS Business/System privacy and security practices which may improve processes and systems involved in collection, use, and maintenance of personally identifiable information (PII). Timely communication and resolution of complaints from individuals demonstrates responsiveness by CMS and the CMS Businesses/Systems and reduces CMS and the CMS Business/System's risk of reputational damage and potential lawsuits under HIPAA and the Privacy Act. CMS and CMS Businesses/Systems should establish a complaint management process that ensures complaints are resolved within a reasonable amount of time.
Privacy Implementation Standards Systems processing, storing, or transmitting PII (to include PHI): High & Moderate: PRIV.1 - Amend control to include: (f) Respond to any appeal as soon as possible, but no later than thirty (30) working days after receipt of the appeal unless the appeal authority can show good cause to extend the response period.
HVA Control Statement
HVA Discussion
HVA Implementation Standard

<table>
<tr><td><b>Control Number</b>
<b>PM-27</b></td><td><b>Control Name</b>
<b>Privacy Reporting</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
(a) Develop privacy reports ,compliant with Federal and HHS Requirements, and disseminate to:
1. OMB, Congress, and other oversight bodies to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and
2. CMS Executive Management (CIO, CISO, CMS Senior Official for Privacy) and other personnel with responsibility for monitoring privacy program compliance; and
(b) Review and update privacy reports CMS define frequency [ODP = monthly]</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Through internal and external reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting can also help organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, discover vulnerabilities, identify gaps in policy and implementation, and identify models for success. Privacy reports include annual senior agency official for privacy reports to OMB; reports to Congress required by Implementing Regulations of the 9/11 Commission Act; and other public reports required by law, regulation, or policy, including internal policies of organizations. The senior agency official for privacy consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.
At CMS, all systems are required to meet privacy reporting requirements. Even if a system does not process, store, or transmit PII, the Mission/Business/System owner must still meet the privacy reporting requirements by submitting a statement that the system does not process, store, or transmit PII.
(g) Issues publicly available guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High, Moderate & Low:
Std.1 - The Senior Official for Privacy (SOP) where PII/PHI is collected for a system will: . 1 - Develop privacy reports ,compliant with Federal and HHS Requirements, and disseminate the reports to:
a. OMB, Congress, and other oversight bodies to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and
b. CMS Executive Management (CIO, CISO, CMS Senior Official for Privacy) and other personnel with responsibility for monitoring privacy program compliance; and
2. Review and update privacy reports CMS monthly.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
IR-9, PM-19;</td><td colspan="2"><b>Reference Policy</b>
Code: 5 U.S.C. §552a, 44 U.S.C. §3541, §3541(4);</td></tr>
</table>

	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208, 9/11 Comm Act: §2000ee-1 Section 803, 2000ee-3 Section 804, Consolidated Appropriations Act §522; FISMA 2014;
	HIPAA: 45 C.F.R. §160.310(a), 45 C.F.R. §164.408;
	OMB Circular: A-108, A-130;
	OMB Memo: M-08-09;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Privacy reporting helps CMS and CMS Businesses/Systems determine progress in meeting privacy compliance requirements and ensure CMS and CMS Business/System accountability. Additionally, the information is used to ensure that CMS is meeting all applicable privacy reporting requirements.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Amend control to include:

(c) The CCIC provides oversight of information security and privacy, to include privacy reporting (e.g., reportable metrics, formats), for each FISMA System operating by or on behalf of CMS.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PM-28	**Risk Framing**	**P2**	**Low** **Moderate** **High**

Control Statement

(a) Identify and document:

1. Assumptions affecting risk assessments, risk responses, and risk monitoring;
2. Constraints affecting risk assessments, risk responses, and risk monitoring;
3. Priorities and trade-offs considered by CMS and, if applicable, the Mission/Business/System for managing risk; and
4. CMS risk tolerance and, if applicable, Mission/Business/System risk tolerance; and

(b) Distribute the results of risk framing activities to CMS Executive Management (CIO, CISO, SOP) and entity-defined personnel (defined in applicable MAC security/privacy plans) ;

(c) Review and update risk framing considerations that does not to exceed ninety (90) days.

Discussion

Risk framing is most effective when conducted at the organization level. The assumptions, constraints, risk tolerance, priorities, and tradeoffs identified as part of the risk framing process, inform the risk management strategy which in turn, informs the conduct of risk assessment, risk response, and risk monitoring activities. Risk framing results are shared with organizational personnel including mission/business owners, information owners or stewards, system owners, authorizing officials, senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management.

Implementation Standard

High, Moderate & Low:

Std.1 - The Risk Management Executive will

1 - Develop the CMS Risk Framing; a set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shapes CMS' approach for managing risk as part of the CMS risk management strategy.

2 - Identify the assumptions, risk, constraints, and trade-offs for the CMS risk tolerance; CMS' or stakeholder’s readiness to bear the risk after risk treatment in order to achieve its objectives.

3 - Share Risk framing results with organizational personnel including mission/business owners, information owners or stewards, system owners, authorizing officials, senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management.	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
CA-7, PM-9, RA-3, RA-7;
	Reference Policy
	NIST SP: 800-39;
	OMB Circular: A-130;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PM-29	**Risk Management Program Leadership Roles**	**P1**	**Low** **Moderate** **High**
Control Statement (a) Appoint a Senior Accountable Official for Risk Management to align CMS information security and privacy management processes with strategic, operational, and budgetary planning processes; and (b) Establish a Risk Executive (function) to view and analyze risk from an Enterprise-wide perspective and ensure management of risk is consistent across CMS.			
Discussion The senior accountable official for risk management leads the risk executive (function) in organization-wide risk management activities.			
Implementation Standard High, Moderate & Low: Std.1 - The CIO and CISO will appoint a Senior Accountable Official for Risk Management, known as the Risk Management Executive, to align the CMS information security and privacy management processes with strategic, operational, and budgetary planning processes to: 1 - Establish a Risk Executive (function) to view and analyze risk from an Enterprise-wide perspective and ensure management of risk is consistent across CMS.			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	
Related Controls PM-2, PM-09, PM-19, PM-28;		**Reference Policy** NIST SP: 800-37;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PM-30	**Supply Chain Risk Management Strategy**	**P1**	**Low** **Moderate** **High**
Control Statement (a) Develop a CMS-wide and, if applicable, Mission/Business/System-wide, strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services; (b) Implement the supply chain risk management strategy consistently across CMS, and if applicable, the Mission/Business/System; and			

(c) Review and update the supply chain risk management strategy that does not exceed three (3) years or as required, to address CMS and/or Mission/Business/System organizational changes.

Discussion

An organization-wide supply chain risk management strategy includes an unambiguous expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management strategy, and the associated roles and responsibilities. Supply chain risk management includes considerations of both security and privacy risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. The supply chain risk management strategy can be incorporated into the organization's overarching risk management strategy and can guide and inform the system-level supply chain risk management plan. The use of a risk executive function can facilitate a consistent, organization-wide application of the supply chain risk management strategy. The supply chain risk management strategy is implemented at the organizational level, whereas the supply chain risk management plan (see SR-2) is applied at the system-level.

Implementation Standard

High, Moderate & Low:

Std.1 - The CIO and CISO will:

1 - Develop a CMS-wide and, if applicable, Mission/Business/System-wide, strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

2 - Implement the supply chain risk management strategy consistently across CMS, and if applicable, the Mission/Business/System; and

3 - Review and update the supply chain risk management strategy that does not exceed three (3) years or as required, to address CMS and/or Mission/Business/System organizational changes.

4 - Assign this objective to the OIT - ISPG - Division of Strategic Information for oversight and management in conjunction with the support of the CCIC for systems identified as critical in the supply chain processes and risk tolerances.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years
Related Controls PM-9, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11;	**Reference Policy** NIST SP: 800-161;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PM-30(01)	**Suppliers of Critical or Mission-Essential Items**	**P1**	**Low** **Moderate** **High**

Control Statement

Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services

Discussion

The identification and prioritization of suppliers of critical or mission-essential technologies, products, and services is paramount to the mission/business success of organizations. The assessment of suppers is conducted using supplier reviews (see SR-6) and supply chain risk assessment processes (see RA-3(1)). An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Implementation Standard

High, Moderate & Low:

Std.1 The CCIC and OIT - ISPG - Division of Strategic Information will perform an analysis of supply chain risk systems or components for which additional supply chain risk mitigations are required.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Three (3) Years

Related Controls RA-3, SR-6	**Reference Policy**
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **PM-31**	**Control Name** **Continuous Monitoring Strategy**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement Develop a CMS Enterprise-wide and, when applicable, a Mission/Business/System-wide continuous monitoring strategy and implement continuous monitoring programs that include: (a) Establishing the following CMS Enterprise-wide metrics and, if applicable, Mission/Business/System-wide metrics, to be monitored: CCIC defined metrics and, (b) Establishing defined frequencies (defined by the CCIC CDM Program), but no less than once every 72 hours for monitoring and defined frequencies (defined by the CCIC CDM Program), but no less than once every 72 hours for assessment of control effectiveness (c) Ongoing monitoring of CMS Enterprise-wide metrics and, if applicable, Mission/Business/System-wide metrics in accordance with the continuous monitoring strategy; (d) Correlation and analysis of information generated by control assessments and monitoring; (e) Response actions to address results of the analysis of control assessment and monitoring information; and (f) Reporting the security and privacy status of Mission/Business/System to defined personnel or roles that does not to exceed thirty (30) days.			
Discussion Continuous monitoring at the organization level facilitates ongoing awareness of the security and privacy posture across the organization to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring guide and inform risk response actions by organizations. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives organizational officials the capability to make effective and timely risk management decisions, including ongoing authorization decisions. Monitoring requirements, including the need for specific monitoring, may be referenced in other controls and control enhancements, for example, AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CA-7, CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PS-7e, SA-9c, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18c, SC-43b, SI-4.			
Implementation Standard High, Moderate & Low: Std.1 The CCIC continuous monitoring strategy guides implementation through the phases of the Information Security Continuous Monitoring (ISCM) program will: Phase 1: What is on the network Phase 2: Who is on the network Phase 3: What is happening on the network Phase 4: Protecting Data on the Network			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	
Related Controls AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CA-7, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PS-7, PT-8, RA-3, RA-5, RA-7, SA-9, SA-11, SC-		**Reference Policy** NIST SP: 800-37, 800-137;	

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **PM-32**	**Control Name** **Purposing**	**Priority** **P2**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement Analyze CMS Mission/Business/System or system components supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.
Discussion Systems are designed to support a specific mission or business function. However, over time, systems and system components may be used to support services and functions that are outside the scope of the intended mission or business functions. This can result in exposing information resources to unintended environments and uses that can significantly increase threat exposure. In doing so, the systems are in turn more vulnerable to compromise, and can ultimately impact the services and functions for which they were intended. This is especially impactful for mission essential services and functions. By analyzing resource use, organizations can identify such potential exposures.
Implementation Standard High, Moderate & Low: Std.1 - The CIO and CISO will: 1 - Perform an analysis of CMS Mission/Business/System(s) or system components supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls CA-7, PL-2, RA-3, RA-9;+AD39	**Reference Policy** NIST SP: 800-137;

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion

Personnel Security

Control Number	Control Name	Priority	CMS Baseline
PS-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

a. Develop, document, and disseminate to applicable personnel or roles:

1. CMS Enterprise-level personnel security policy that:
    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:

1. Policy at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

Personnel security policy and procedures for the controls in the PS family that are implemented within systems and at the CMS Enterprise-level. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to personnel security policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure

CMS provides an enterprise level personnel security policy within this ARS, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures).

Implementation Standard

High, Moderate & Low:

Std.1 - The CIO and CISO will provide leadership and oversight to:

a. Develop, document, and disseminate to applicable personnel or roles:

1. CMS Enterprise-level, Mission/Business process-level and System-level personnel security policy that:
    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:

1. Policy at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
PM-9, PS-8, SI-12.
	Reference Policy
	FedRAMP Rev. 4 Baseline;
	FISCAM: AS-1, SM-1, SM-3, SM-4;
	HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(3)(ii)(C); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(ii)
	NIST SP: 800-12, 800-30, 800-39, 800-100;
	OMB Memo: M-17-12, Att. 4;
	OMB Circular A-130: 7.g. and 8.a.1(f)

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Roles that require access to certain types of sensitive information, such as PII may require additional personnel security measures beyond those applied to the general workforce of an organization. This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PS-02	**Position Risk Designation**	**P1**	**Low** **Moderate** **High**

Control Statement

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions;

c. Ensure that all individuals with significant security responsibilities possess, at a minimum, a Level-5 Public Trust;

d. Ensure that individuals are designated to position-sensitivity levels that are commensurate with the responsibilities and risks associated with the position; and

e. Review and update position risk designations at least within three years or whenever a position’s duties are changed/revised/realigned, and ensure that these risk designations are consistent with the OPM Position Designation Automated Tool (PDT), the HHS Personnel Security/Suitability Handbook, and the guidance in the CMS Personnel Security Policy.

Discussion

Position risk designations reflect Office of Personnel Management (OPM) policy and guidance. Proper position designation is the foundation of an effective and consistent suitability and personnel security program. The Position Designation System (PDS) assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the service due to misconduct of an incumbent of a position and establishes the risk level of that position. The PDS assessment also determines if the duties and responsibilities of the position present the potential for position incumbents to bring about a material adverse effect on national security and the degree of that potential effect, which establishes the sensitivity level of a position. The results of the assessment determine what level of investigation is conducted for a position. Risk designations can guide and inform the types of authorizations that individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements. Parts 1400 and 731 of Title 5, Code of Federal Regulations, establish the requirements for organizations to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions.

Implementation Standard

High, Moderate & Low:

Std.1 - Ensure all individuals with significant security responsibilities possess, at a minimum, a Level 5 Public Trust;

Std. 2 - Ensure that individuals are designated to position-sensitivity levels that are commensurate with the responsibilities and risks associated with the position. (All employees and contractors approved for a personnel security/suitability level must continue to maintain the security/suitability standards and comply with HHS security policies during their tenure in the position).

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA-21, SI-12	**Reference Policy** 5 CFR 731; NIST: SP 800-181.

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Position risk designations, for different levels of access to sensitive information such as PII should be commensurate with the risks associated with the confidentiality impact level for the information.

Discussion for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PS-03	**Personnel Screening**	**P1**	**Low** **Moderate** **High**

Control Statement

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with OPM, HHS, and the CMS Personnel Security Policy and whenever individuals move to a new position with a higher risk designation and where rescreening is indicated.;

c. Conduct background investigations in a manner commensurate with the HHS Personnel Security/Suitability Handbook and the CMS Personnel Security policy and guidance.

d. Perform reinvestigations in accordance with guidance provided by HHS and the current CMS Personnel Security Policy; and

e. Refuse employees and contractors access to information systems until they have:

1. Been vetted in accordance with agency policy; and
2. Signed the appropriate access agreements.

Discussion

Personnel screening and rescreening activities reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and specific criteria established for the risk designations of assigned positions. Examples of personnel screening include background investigations and agency checks. Organizations may define different rescreening conditions and frequencies for personnel accessing systems based on types of information processed, stored, or transmitted by the systems.

Implementation Standard

High, Moderate & Low:

Std.1 - Require that individuals with significant security responsibilities be assigned and hold, at a minimum, a Level 5 Public Trust background investigation as defined by HHS and CMS Personnel Security Policy.

Std. 2 - Conduct background investigations in a manner commensurate with HHS and the CMS Personnel Security policy and guidance;

Std. 3 - Perform reinvestigations in accordance with guidance provided by current CMS Personnel Security Policy; and

Std. 4 - Refuse employees and contractors access to information systems until they have:

1. Been vetted in accordance with agency policy; and
2. Signed the appropriate access agreements.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years

Related Controls	Reference Policy

AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21.	EO: 13526, 13587;
	FIPS: 199, 201-2;
	SP: 800-60-1, 800-60-2, 800-73-4, 800-76-2, 800-78-4.

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Screening individuals who are provided access to sensitive information, such as PII, and re-screening as deemed appropriate by CMS or the organization, reduces risk.

Discussion for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Privacy Implementation Standards

High, Moderate & Low:

PRIV.1 - a. Require that individuals with significant security responsibilities be assigned and hold, at a minimum, a Level 5 Public Trust background investigation as defined in the HHS Personnel Security/Suitability Handbook.

b. Assign other individuals with Public Trust positions the appropriate sensitivity level as defined in the HHS Personnel Security/Suitability Handbook.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PS-03(04)	**Citizenship Requirements**		**Above Baseline**

Control Statement

Verify that individuals accessing a system processing, storing, or transmitting sensitive CMS-information types meet citizenship requirements consistent with the HHS Personnel Security/Suitability Handbook and the CMS Personnel Security Policy.

Discussion

None.

Implementation Standard

Control Review Frequency	Assessment Frequency
Not Specified	Three (3) Years

Related Controls	Reference Policy

	EO 13526, 13587;
	FIPS 199, 201-2;
	NIST: SP 800-60-1, 800-60-2, 800-73-4, 800-76-2, 800-78-4;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PS-04	**Personnel Termination**	**P2**	**Low** **Moderate** **High**

Control Statement

Upon termination of individual employment:
a. Disable system access within Implementation Standard 1;
b. Terminate or revoke any authenticators and credentials associated with the individual;
c. Conduct exit interviews that include a discussion of non-disclosure of information security and privacy information;
d. Retrieve all security-related organizational system-related property; and
e. Retain access to organizational information and systems formerly controlled by terminated individual;
f. Notify defined personnel or roles (defined in the applicable security plan) within one (1) calendar day; and
g. Immediately escorts employees terminated for cause out of the organization, when applicable.

Discussion

System property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics at exit interviews include reminding individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not always be possible for some individuals, including in cases related to the unavailability of supervisors, illnesses, or job abandonment. Exit interviews are important for individuals with security clearances. The timely execution of termination actions is essential for individuals who have been terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals who are being terminated prior to the individuals being notified.

Implementation Standard

High, Moderate, & Low:
Std.1 - System access must be disabled prior to or during the employee termination process/action
Std.2 - All access and privileges to systems, networks, and facilities are suspended when employees or contractors temporarily separate from the organization (e.g., leave of absence).

Control Review Frequency	Assessment Frequency
Monthly	Annually (365 Days)
Related Controls	**Reference Policy**
AC-2, IA-4, PE-2, PM-12, PS-6, PS-7	None.

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
This control governs termination procedures for access to sensitive information, such as personally identifiable information (PII).
Discussion for systems processing, storing, or transmitting PHI:
Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **PS-04(01)**	**Control Name** **Post-Employment Requirements**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement a. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and b. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.			
Discussion Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None		**Reference Policy** None	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **PS-04(02)**	**Control Name** **Automated Actions**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Use automated mechanisms (defined in system security and privacy plan) to notify appropriate personnel or roles (defined in the applicable security and privacy plan, e.g. HR, Managers, Supervisors, COR, System Administrators, Physical Security Personnel) of individual termination actions; disable access to system resources.			
Discussion In organizations with many employees, not all personnel who need to know about termination actions receive the appropriate notifications, or if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to organizational personnel or roles when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including via telephone, electronic mail, text message, or websites. Automated mechanisms can also be employed to quickly and thoroughly disable access to system resources after an employee is terminated.			
Implementation Standard High: Std.1 - If automated mechanisms are not feasible, a manual and documented process must be in place by notifying defined personnel or roles (defined in the applicable security and privacy plan, e.g. HR, Managers, Supervisors, COR, System Administrators, Physical Security Personnel) within seven (7) calendar days of the individual’s termination.			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	
Related Controls None;		**Reference Policy** None.	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number	Control Name	Priority	CMS Baseline
PS-05	**Personnel Transfer**	**P2**	**Low** **Moderate** **High**

Control Statement

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiate the following transfer or reassignment actions during the formal transfer process as soon as possible but no later than 30 days:
1. Re-issuing or confirming the need to continue to have/access appropriate information system-related property (e.g., keys, identification cards, building passes);
2. Notifying security management;
3. Closing obsolete accounts and establishing new accounts; and
4. When an employee moves to a new position of trust, re-evaluating logical and physical access controls
c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notify appropriate personnel or roles (defined in the applicable security and privacy plan, e.g. HR, Managers, Supervisors, COR, System Administrators, Physical Security Personnel) within (7) calendar days.

Discussion

Personnel transfer applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

Implementation Standard

High, Moderate & Low:
Std. 1 - Revoke employee access rights immediately upon notification of the transfer. Physical access is revoked immediately following employee transfer, and procedures are in place to ensure system access is revoked prior to or during the employee transfer process.

Control Review Frequency	Assessment Frequency
Monthly	Annually (365 Days)

Related Controls	Reference Policy

AC-2, IA-4, PE-2, PM-12, PS-4, PS-7.	Code: 5 U.S.C. §552a(b)(1) and (e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-4;
	HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(C), 45 C.F.R. §164.308(a)(3)(ii)(B);

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
When personnel are reassigned or transferred, their access to sensitive information, such as PII, must be reviewed to determine whether and how their access permissions should change.
Discussion for systems processing, storing, or transmitting PHI:
Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Privacy Implementation Standards

High, Moderate & Low:
PRIV.1 - Individuals that work with personally identifiable information (PII) are screened prior to being provided access to the PII and re-screened as determined by the organization.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PS-06	**Access Agreements**	**P3**	**Low** **Moderate** **High**

Control Statement

a. Develop and document access agreements for organizational systems;
b. Review and update the access agreements within every 365 days; and
c. Verify that individuals requiring access to organizational information and systems:
1. Sign appropriate access agreements (paper or electronic) prior to being granted access; and
2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or within every 365 days.

Discussion

Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.
The HHS RoB is the standard HHS access agreement. All new users of HHS, including CMS, information resources must read the HHS RoB and sign the accompanying acknowledgement form before accessing Department data or other information, systems, and/or networks. This acknowledgement must be completed every 365 days thereafter, which may be done as part of annual the organization Information Systems Security Awareness Training (see AT-3).

Implementation Standard

High, Moderate & Low:
Std.1 - Develop and document the access agreements for CMS systems.
Std.2 - Review, update, and verify that individuals requiring access to organizational systems sign the appropriate access agreements.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)
Related Controls	**Reference Policy**

AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SA-21, SI-12.
(Redacted Privacy Controls: AR-5)
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, AS-4, SD-1, SD-2, SM-4;
	HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(3)(ii)(B), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.310(b), 45 C.F.R. §164.310(d)(2)(iii), 45 C.F.R. §164.314(a)(1), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(ii), 45 C.F.R. §164.314(a);
	OMB Memo: M-17-12 Att. 1 A.2. and Att. 4;

Privacy Discussion

Guidance for systems processing, storing, or transmitting PII (to include PHI):
Examples of access agreement documents required for access to personally identifiable information (PII) may include access authorization requests, nondisclosure agreements, acceptable use agreements, privacy training and awareness, and rules of behavior.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PS-07	**External Personnel Security**	**P1**	**Low** **Moderate** **High**

Control Statement

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;
c. Document personnel security requirements;
d. Require external providers to notify Contracting Officers or Contracting Officer Representatives (via the roster of contractor personnel) of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within a maximum of seven-two (72) hours for systems designated as High impact; seven (7) calendar days for systems designated as Moderate impact, or thirty (30) calendar days for systems designated as Low impact, from the formal termination action; and
e. Monitor provider compliance with personnel security requirements.

Discussion

External provider refers to organizations other than the organization operating or acquiring the system. External providers include service bureaus, contractors, and other organizations that provide system development, information technology services, testing or assessment services, outsourced applications, and network/security management. Organizations explicitly include personnel security requirements in acquisition-related documents. External providers may have personnel working at organizational facilities with credentials, badges, or system privileges issued by organizations. Notifications of external personnel changes ensure the appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include functions, roles, and the nature of credentials or privileges associated with transferred or terminated individuals.

Implementation Standard

High, Moderate & Low:
Std.1 - Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access and must agree to and support the information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support information security policies and standards.

Control Review Frequency	**Assessment Frequency**
Monthly	Annually (365 Days)
Related Controls	**Reference Policy**

AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA-9, SA-21.
(Redacted Privacy Controls: AR-3)
	Code: 5 U.S.C. §552a(m);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	Federal Acquisition Regulation (FAR): Parts 24.1, 39.105, 52.224-1&2;
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-4, SM-7;
	HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.308(b)(1), 45 C.F.R. §164.314(a)(1), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(ii), 45 C.F.R. §164.314(a);
	NIST SP: 800-35, 800-63-3;
	OMB Circular: A-130 7.g. 8.a.1(f);

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):
This control ensures that external providers that will have access to sensitive information, such as personally identifiable information (PII), are held accountable in the same way the organizational personnel are held accountable.

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **PS-08**	**Control Name** **Personnel Sanctions**	**Priority** **P3**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement

a. Employ a formal sanctions process (that may include termination of employment; removal or disbarment from work on federal contracts or projects; suspension of access privileges; revocation of access to federal information, information systems and/or facilities; criminal penalties) for individuals failing to comply with established information security and privacy policies and procedures; and

b. Notify appropriate personnel or roles (defined in the applicable security and privacy plan, e.g. HR, Managers, Supervisors, COR, Physical Security Personnel) not to exceed seven-two (72) hours for systems designated as High impact; seven (7) calendar days for systems designated as Moderate impact; and thirty (30) calendar days for systems designated as Low impact when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Discussion

Organizational sanctions reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Sanctions processes are described in access agreements and can be included as part of general personnel policies for organizations and/or specified in security and privacy policies. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

Implementation Standard

High, Moderate & Low:

Std.1 Administer disciplinary action against CMS employees in accordance with the provisions of 5 USC Chapter 75 (statutory requirements for taking adverse actions), 5 CFR Part 752 (regulatory requirements for taking adverse actions), HHS Instructions (Reprimands), and the procedures set out in Article 23 of the Master Labor Agreement16 (MLA) between CMS and the American Federation of Government Employees, Local 1923 (bargaining unit employees only).

Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)

Related Controls
All XX-1 Controls, PL-4, PM-12, PS-6, PT-1.
	Reference Policy
	Code: 5 U.S.C. §552a(e)(9);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-4;
	HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(C);
	OMB Memo: M-17-12 Att. 2 A.2. Att. 4;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

If the personnel sanctions are associated with the loss, theft, or compromise of personally identifiable information (PII), additional care must be taken to prevent further privacy incidents. When providing notice of sanctions, do not provide the PII involved in the incident to anyone without an explicit need to know. Unless the individual needs the specific PII elements breached to perform their job function, the individual does not need to know the PII. Instead, provide characterization of the type(s) of PII breached (e.g., provide “Full Name” instead of providing “John Doe,” or “Blood Type” instead of “A positive”).

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **PS-09**	**Control Name** **Position Descriptions**	**Priority**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement

Incorporate security and privacy roles and responsibilities into organizational position descriptions (Security and privacy responsibilities identified in the HHS IS2P and CMS IS2P2)	
Discussion Specification of security and privacy roles in individual organizational position descriptions facilitates clarity in understanding the security or privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls None	**Reference Policy** NIST SP: 800-181
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Personally Identifiable Information Processing and Transparency

Control Number	Control Name	Priority	CMS Baseline
PT-01	**Policy and Procedures**	**P1**	**Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel and roles:

1. CMS Enterprise-level personally identifiable information processing and transparency policy that:
   a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and

(c) Review and update the current personally identifiable information processing and transparency:

1. Policy at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

This control addresses policy and procedures for the controls in the PT family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise level access control policy within this ARS, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures.)

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**
None;	OMB Circular: A-130;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PT-02	**Authority to Process Personally Identifiable Information**	**P1**	**Moderate** **High**

Control Statement

Systems processing, storing, or transmitting PII (to include PHI):
(a) Determine and document the relevant legal authority (defined in applicable security/privacy plans) that permits the collection, use, maintenance, and sharing of personally identifiable information, either generally or in support of CMS specific missions, businesses, and programs; and
(b) Restrict the minimum relevant and necessary elements (defined in applicable security/privacy plans) of personally identifiable information to only that which is authorized.

Discussion

Processing of personally identifiable information is an operation or set of operations that the information system or organization performs with respect to personally identifiable information across the information life cycle. Processing includes, but is not limited to, creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining.

CMS Businesses/Systems may be subject to laws, executive orders, directives, regulations, or policies that establish the organization's authority and thereby limit certain types of processing of personally identifiable information or establish other requirements related to the processing. CMS Businesses/Systems personnel consult with the senior agency official for privacy and legal counsel regarding such authority, particularly if the organization is subject to multiple jurisdictions or sources of authority. For organizations whose processing is not determined according to legal authorities, the organizations' policies and determinations govern how they process personally identifiable information. While processing of personally identifiable information may be legally permissible, privacy risks may still arise from its processing. Privacy risk assessments can identify the privacy risks associated with the authorized processing of personally identifiable information and support solutions to manage such risks.

CMS Businesses/Systems consider applicable requirements and organizational policies to determine how to document this authority. For federal agencies, the authority to process personally identifiable information is documented in privacy policies and notices, system of records notices, privacy impact assessments, Privacy Act statements, computer matching agreements and notices, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

CMS Businesses/Systems take steps to ensure that personally identifiable information is processed only for authorized purposes, including training organizational personnel on the authorized processing of personally identifiable information and monitoring and auditing organizational use of personally identifiable information.

Before collecting PII, CMS Businesses/Systems must determine whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Official for Privacy (SOP), and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN), Privacy Impact Assessment (PIA), and/or other applicable documentation such as Privacy Act Statements, Notices of Privacy Practices, Website Privacy Policies, or Computer Matching Agreements.

CMS Businesses/Systems must ensure PII collected, used, maintained, or disseminated is related to, and compatible with, the purpose and scope of the authority described in the information system documentation, including privacy documentation such as a SORN or PIA when applicable.

Implementation Standard

Control Review Frequency	**Assessment Frequency**
Three (3) Years	Three (3) Years
Related Controls	**Reference Policy**

AC-2, AC-3, CM-13, PM-9, PM-24, PT-1, PT-3, PT-6, PT-7, RA-3, RA-8, SI-12, SI-18;	Code: 5 U.S.C. §552a;
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208;
	OMB Circular: A-130 Appendix I & Appendix II;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PT-03	**Personally Identifiable Information Processing Purposes**	**P1**	**Moderate** **High** **HVA**

Control Statement

Systems processing, storing, or transmitting PII (to include PHI):
(a) Identify and document the CMS Mission/Business/System-defined purpose(s) (defined in applicable system security/privacy plans) for processing personally identifiable information;

(b) Describe the purpose(s) in the public privacy notices and policies (e.g., via PIAs, SORNs, Privacy Act Statements, and Computer Matching Agreements [CMAs]) published by CMS and the CMS Mission/Business/System;
(c) Restrict the CMS Mission/Business/System-defined processing (defined in applicable system security/privacy plans) of personally identifiable information to only that which is compatible with the identified purpose(s); and
(d) Monitor changes in processing personally identifiable information and implement CMS Mission/Business/System-defined mechanisms (defined in applicable system security plan security/privacy plans) to ensure that any changes are made in accordance with CMS Mission/Business/System-defined requirements.

Discussion

Identifying and documenting the purpose for processing provides organizations with a basis for understanding why personally identifiable information may be processed. The term process includes every step of the information life cycle, including creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Identifying and documenting the purpose of processing is a prerequisite to enabling owners and operators of the system, and individuals whose information is processed by the system, to understand how the information will be processed. This enables individuals to make informed decisions about their engagement with information systems and organizations, and to manage their privacy interests. Once the specific processing purpose has been identified, the purpose is described in the organization’s privacy notices, policies, and any related privacy compliance documentation, including privacy impact assessments, system of records notices, Privacy Act statements, computer matching notices, and other applicable Federal Register notices.

CMS Businesses/Systems take steps to help ensure that personally identifiable information is processed only for identified purposes, including training organizational personnel and monitoring and auditing organizational processing of personally identifiable information.

CMS Businesses/Systems monitor for changes in personally identifiable information processing. CMS Businesses/Systems personnel consult with the senior agency official for privacy and legal counsel to ensure that any new purposes arising from changes in processing are compatible with the purpose for which the information was collected, or if the new purpose is not compatible, implement mechanisms in accordance with defined requirements to allow for the new processing, if appropriate. Mechanisms may include obtaining consent from individuals, revising privacy policies, or other measures to manage privacy risks arising from changes in personally identifiable information processing purposes.

CMS Businesses/Systems must ensure PII collected, used, maintained, or disseminated is related to, and compatible with, the purpose and scope of the authority described in the information system documentation, including privacy documentation such as a SORN or PIA when applicable.

Implementation Standard

Control Review Frequency	**Assessment Frequency**
Three (3) Years	Three (3) Years

Related Controls	**Reference Policy**

AC-2, AC-3, AT-3, CM-13, PM-9, PM-25, PT-2, PT-6, PT-7, PT-8, RA-8, SC-43, SI-12, SI-18;	Code: 5 U.S.C. §552a(e)(3)(A)-(B);
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208(b)(2)(B)(ii) and (c)(1)(B);
	OMB Circular: A-130 Appendix II;

Privacy Discussion

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
High & Moderate:
PRIV.1 - All PII must be used for an official government purpose only. The officers and employees of CMS and CMS Lines of Business and Systems must have a need for the PII in the performance of their official duties. These requirements apply to all PII regardless of its coverage by the Privacy Act.

HVA Control Statement

Systems processing, storing, or transmitting PII (to include PHI):
(a) Identify and document the CMS Mission/Business/System-defined purpose(s) (defined in applicable MAC system security/privacy plans) for processing personally identifiable information;
(b) Describe the purpose(s) in the public privacy notices and policies (e.g., via PIAs, SORNs, Privacy Act Statements, and Computer Matching Agreements [CMAs]) published by CMS and the CMS Mission/Business/System;
(c) Restrict the CMS Mission/Business/System-defined processing (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans) of personally identifiable information to only that which is compatible with the identified purpose(s); and
(d) Monitor changes in processing personally identifiable information and implement CMS Mission/Business/System-defined mechanisms (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans) to ensure that any changes are made in accordance with CMS Mission/Business/System-defined requirements.

HVA Discussion

Identifying and documenting the purpose for processing provides organizations with a basis for understanding why personally identifiable information may be processed. The term process includes every step of the information life cycle, including creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Identifying and documenting the purpose of processing is a prerequisite to enabling owners and operators of the system, and individuals whose information is processed by the system, to understand how the information will be processed. This enables individuals to make informed decisions about their engagement with information systems and organizations, and to manage their privacy interests. Once the specific processing purpose has been identified, the purpose is described in the organization's privacy notices, policies, and any related privacy compliance documentation, including privacy impact assessments, system of records notices, Privacy Act statements, computer matching notices, and other applicable Federal Register notices.

CMS Businesses/Systems take steps to help ensure that personally identifiable information is processed only for identified purposes, including training organizational personnel and monitoring and auditing organizational processing of personally identifiable information.

CMS Businesses/Systems monitor for changes in personally identifiable information processing. CMS Businesses/Systems personnel consult with the senior agency official for privacy and legal counsel to ensure that any new purposes arising from changes in processing are compatible with the purpose for which the information was collected, or if the new purpose is not compatible, implement mechanisms in accordance with defined requirements to allow for the new processing, if appropriate. Mechanisms may include obtaining consent from individuals, revising privacy policies, or other measures to manage privacy risks arising from changes in personally identifiable information processing purposes.

CMS Businesses/Systems must ensure PII collected, used, maintained, or disseminated is related to, and compatible with, the purpose and scope of the authority described in the information system documentation, including privacy documentation such as a SORN or PIA when applicable.

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PT-04	**Consent**	**P1**	**Moderate** **High**

Control Statement

Systems processing, storing, or transmitting PII (to include PHI):

Implement legally sufficient means (defined in applicable system security/privacy plans) for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making

Discussion

Consent allows individuals to participate in the decision-making about the processing of their information and transfers some of the risk that arises from the processing of personally identifiable information from the organization to an individual. Organizations consider whether other controls may more effectively mitigate privacy risk either alone or in conjunction with consent. Consent may be required by applicable laws, executive orders, directives, regulations, policies, standards, or guidelines. Otherwise, when selecting this control, organizations consider whether individuals can be reasonably expected to understand and accept the privacy risks arising from their authorization. Organizations also consider any demographic or contextual factors that may influence the understanding or behavior of individuals with respect to the data actions carried out by the system or organization. When soliciting consent from individuals, organizations consider the appropriate mechanism for obtaining consent, including how to properly authenticate and identity proof individuals and how to obtain consent through electronic means. In addition, organizations consider providing a mechanism for individuals to revoke consent once it has been provided, as appropriate. Finally, organizations consider usability factors to help individuals understand the risks being accepted when providing consent, including the use of plain language and avoiding technical jargon.

Individual participation and agreement to provide information is fundamental to an individual making an informed decision regarding the collection, use, and safeguarding of their PII. To obtain consent, CMS and CMS Businesses/Systems must provide individuals an appropriate notice of the purposes for which the PII is collected, how the PII will be used, and a means for the individual to consent to or decline the activity. CMS and CMS Businesses/Systems must tailor the public notice and consent mechanisms to meet their operational needs. Consent mechanisms should include a discussion of any consequences should an individual fail to provide the needed PII.

CMS and CMS Businesses/Systems may obtain consent through opt-in, opt-out, or implied consent:

- Opt-in consent is the preferred method, but may not always be feasible. (Opt-in requires individuals take affirmative action to allow the collection and use of their PII.)
- Opt-out requires individuals take specific action to prevent the new or continued collection (i.e., disallow) of their PII.
- Implied consent should be used only in limited circumstances where both opt-in and opt-out are not feasible options. Implied consent occurs where an individuals' behavior, or failure to object, indicates agreement with the collection or use of PII.

Whenever feasible, opt-in is the preferred method to obtain consent.

Implementation Standard	
Control Review Frequency Three (3) Years	**Assessment Frequency** Three (3) Years

Related Controls
AC-16, PT-2, PT-5
	Reference Policy
	Code: 5 U.S.C. §552a(b), 5 U.S.C. §552a(e)(3)-(4);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	NIST SP: 800-63-3;
	OMB Circular: A-130 Appendix II;
	OMB Memo: M-03-22, M-10-22;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
PT-05	**Privacy Notice**	**P1**	**Moderate** **High**

Control Statement

Systems processing, storing, or transmitting PII (to include PHI):

Provide notice to individuals about the processing of personally identifiable information that:

(a) Is available to individuals upon first interacting with an organization, and subsequently at times prescribed by law or more often as the organization deems);

(b) Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;

(c) Identifies the authority that authorizes the processing of personally identifiable information;

(d) Identifies the purposes for which personally identifiable information is to be processed; and

(e) Includes the following information at a minimum.

1. How PII is protected;
2. Activities impacting privacy, to include collection, use, sharing, safeguarding, maintenance, and disposal of PII, and how the PII will be used internally;
3. If PII is shared PII with external entities, how those entities are categorized, and the purposes for such sharing;
4. Choices individuals may have regarding how their PII may be used (i.e., consent to specific uses or sharing) and the consequences of exercising or not exercising those choices; and
5. Ability to access and have PII amended or corrected if and when necessary.

Discussion

Privacy notices help inform individuals about how their personally identifiable information is being processed by the system or organization. Organizations use privacy notices to inform individuals about how, under what authority, and for what purpose their personally identifiable information is processed, as well as other information such as choices individuals might have with respect to that processing and, other parties with whom information is shared. Laws, executive orders, directives, regulations, or policies may require that privacy notices include specific elements or be provided in specific formats. Federal agency personnel consult with the senior agency official for privacy and legal counsel regarding when and where to provide privacy notices, as well as elements to include in privacy notices and required formats. In circumstances where laws or government-wide policies do not require privacy notices, organizational policies and determinations may require privacy notices and may serve as a source of the elements to include in privacy notices.

Privacy risk assessments identify the privacy risks associated with the processing of personally identifiable information and may help organizations determine appropriate elements to include in a privacy notice to manage such risks. To help individuals understand how their information is being processed, organizations write materials in plain language and avoid technical jargon.

Providing the appropriate notification of privacy practices to the individual enables the individual to make an informed decision when they provide their consent. Additionally, changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SOP and Chief Counsel. The website privacy policy, per OMB M-17-12, Policies for Federal Agency Public Websites and Digital Services, frequently referred to on organization websites as a “Privacy Policy” or “Privacy and Security

Notice,” is intended as a broad notice of website privacy policies and general website use, and will not by itself meet the requirement for specific notice when collecting PII. When PII is maintained (including collection) in a system of records that is covered by the Privacy Act, the organization must provide a “Privacy Act Statement” to the individual at the time of collection that meets the requirements of the Privacy Act of 1974, 5 U.S.C. §552a(e)(3), unless the organization has published a rule exempting that system of records from the (e)(3) notice provision in accordance with subsection (j) of the Privacy Act. If the PII is not maintained in a system of records under the Privacy Act, a privacy notice should be provided which describes the privacy practices associated with that PII, including, but not limited to, the way the PII is protected, how it is used, and whether it is shared. To avoid confusion, this type of privacy notice must not be labeled as a “Privacy Act Statement.” As an alternative, several organizations refer to this notice type as a “Privacy Advisory.”

Implementation Standard

Control Review Frequency Three (3) Years	**Assessment Frequency** Three (3) Years

Related Controls
PM-20, PM-22, PT-2, PT-3, PT-4, PT-7, RA-3, SI-18;
	Reference Policy
	Statute: Privacy Act of 1974 (P.L. 93-579);
	NIST SP: 800-63-3;
	OMB Circular: A-108, A-130;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
PT-05(02)	**Privacy Act Statements**	**P1**	**Moderate** **High**

Control Statement

Systems processing, storing, or transmitting PII (to include PHI):

In coordination with the HHS Privacy Act Officer, the CMS SOP, CMS Privacy Contacts, and the HHS and CMS Offices of General Counsel, includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Discussion

If a federal agency asks individuals to supply information that will become part of a system of records, the agency is required to provide a Privacy Act statement on the form used to collect the information or on a separate form that can be retained by the individual. The agency provides a Privacy Act statement in such circumstances regardless of whether the information will be collected on a paper or electronic form, on a website, on a mobile application, over the telephone, or through some other medium. This requirement ensures that the individual is provided with sufficient information about the request for information to make an informed decision on whether or not to respond.

Privacy Act statements provide formal notice to individuals of the authority that authorizes the solicitation of the information; whether providing the information is mandatory or voluntary; the principal purpose(s) for which the information is to be used; the published routine uses to which the information is subject; the effects on the individual, if any, of not providing all or any part of the information requested; and an appropriate citation and link to the relevant system of records notice. Federal agency personnel consult with the senior agency official for privacy and legal counsel regarding the notice provisions of the Privacy Act.

CMS Businesses/Systems must ensure PII collected, used, maintained, or disseminated is related to, and compatible with, the purpose and scope of the authority described in the information system documentation, including privacy documentation such as a SORN or PIA when applicable.

Implementation Standard

Control Review Frequency Three (3) Years	**Assessment Frequency** Three (3) Years

Related Controls
PT-6
	Reference Policy
	Code: 5 U.S.C. §552a;
	Statute: Privacy Act of 1974 (P.L. 93-579);

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion
HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PT-06	**System of Records Notice**	**P1**	**Moderate** **High**

Control Statement

Systems processing, storing, or transmitting PII (to include PHI):

For systems that process information that will be maintained in a Privacy Act system of records and in coordination with the HHS Privacy Act Officer, the CMS SOP, CMS Privacy Contacts, and the HHS and CMS Offices of General Counsel:

(a) Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;

(b) Publish system of records notices in the Federal Register; and

(c) Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

Discussion

The Privacy Act requires that federal agencies publish a system of records notice in the Federal Register upon the establishment and/or modification of a Privacy Act system of records. As a general matter, a system of records notice is required when an agency maintains a group of any records under the control of the agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier. The notice describes the existence and character of the system, and identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system as described in OMB Circular A-108.

Note: Publication of a SORN in the Federal Register requires a mandatory review and comment period of a minimum of 40 days.

SORNs and Privacy Act Statements, i.e., (e)(3) notices, provide transparency, in advance of collection, use, maintenance, or sharing of PII when in a system that meets the statutory definition of a “system of records” under the Privacy Act. The Privacy Act notes that the Act uses “maintain” to include “maintain, collect, use or disseminate.” Privacy Act requirements impact decisions made during planning, design, development, and operation of programs and systems.

CMS and CMS Businesses/Systems issue SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as “a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or another identifier.” SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. Privacy Act Statements provide notice of:

(i) the authority of organizations to collect PII;

(ii) whether providing PII is mandatory or optional;

(iii) the principal purpose(s) for which the PII is to be used;

(iv) the intended disclosures (routine uses) of the information; and

(v) the consequences of not providing all or some portion of the information requested.

When information is collected verbally, CMS and CMS Businesses/Systems must read a Privacy Act Statements prior to initiating the collection of PII (for example, when conducting telephone interviews or surveys).

The publication of a SORN is required only when PII is maintained in a system that meets the statutory definition of a “system of records” under the Privacy Act. Not all systems containing PII may meet the definition of a “system of records.” However, all PII maintained by an organization must be protected irrespective of whether the PII is subject to the Privacy Act. The Privacy Act Statement, when required, should be provided in the same format as the information is collected. For example, an electronic statement on a website, a written statement on a paper form, and a verbal statement provided for information that is collected verbally.

Implementation Standard

Control Review Frequency	**Assessment Frequency**
Three (3) Years	Three (3) Years
Related Controls	**Reference Policy**
AC-3, PM-20, PT-2, PT-3, PT-5;	Statute: Privacy Act of 1974 (P.L. 93-579);

	NIST SP: 800-63-3;
	OMB Circular: A-108;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **PT-06(01)**	**Control Name** **Routine Uses**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Systems processing, storing, or transmitting PII (to include PHI): Review all routine uses published in the system of records notice at [CMS Entity-Defined: Mission/Business/System]-defined frequency (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans) to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.			
Discussion A Privacy Act routine use is a particular kind of disclosure of a record outside of the federal agency maintaining the system of records. A routine use is an exception to the Privacy Act prohibition on the disclosure of a record in a system of records without the prior written consent of the individual to whom the record pertains. To qualify as a routine use, the disclosure must be for a purpose that is compatible with the purpose for which the information was originally collected. The Privacy Act requires agencies to describe each routine use of the records maintained in the system of records, including the categories of users of the records and the purpose of the use. Agencies may only establish routine uses by explicitly publishing them in the relevant system of records notice.			
Implementation Standard			
Control Review Frequency Three (3) Years		**Assessment Frequency** Three (3) Years	
Related Controls None;		**Reference Policy** See PT-6;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **PT-06(02)**	**Control Name** **Exemption Rules**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Systems processing, storing, or transmitting PII (to include PHI): Review all Privacy Act exemptions claimed for the system of records at [CMS Entity-Defined: Mission/Business/System]-defined frequency (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans) to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.			
Discussion The Privacy Act includes two sets of provisions that allow federal agencies to claim exemptions from certain requirements in the statute. These provisions allow agencies in certain circumstances to promulgate regulations to exempt a system of records from select provisions of the Privacy Act. At a minimum, organizations' Privacy Act exemption			

regulations include the specific name(s) of any system(s) of records that will be exempt, the specific provisions of the Privacy Act from which the system(s) of records is to be exempted, the reasons for the exemption, and an explanation for why the exemption is both necessary and appropriate.	
Implementation Standard	
Control Review Frequency Three (3) Years	**Assessment Frequency** Three (3) Years
Related Controls None;	**Reference Policy** See PT-6;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
PT-07	**Specific Categories of Personally Identifiable Information**	**P1**	**Moderate** **High**

Control Statement Systems processing, storing, or transmitting PII (to include PHI): Apply organization-defined processing conditions for specific categories of personally identifiable information, as identified by the Authorizing Official, CISO, SOP, and in coordination with individual CMS information systems [for specific categories of personally identifiable information.	
Discussion Organizations apply any conditions or protections that may be necessary for specific categories of personally identifiable information. These conditions may be required by laws, executive orders, directives, regulations, policies, standards, or guidelines. The requirements may also come from organizational policies and determinations when an organization has determined that a particular category of personally identifiable information is particularly sensitive or raises particular privacy risks. Organizations consult with the senior agency official for privacy and legal counsel regarding any protections that may be necessary.	
Implementation Standard	
Control Review Frequency Three (3) Years	**Assessment Frequency** Three (3) Years

Related Controls
IR-9, PT-2, PT-3, RA-3
	Reference Policy
	Statute: Privacy Act of 1974 (P.L. 93-579);
	OMB Circular: A-108, A-130;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
PT-07(01)	**Social Security Numbers**	**P1**	**Moderate** **High**

Control Statement Systems processing, storing, or transmitting PII (to include PHI): When a system processes Social Security numbers: (a) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier; (b) Do not deny any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his or her Social Security number; and

(c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.	
Discussion Federal law and policy establish specific requirements for organizations' processing of Social Security numbers. Organizations take steps to eliminate unnecessary uses of Social Security numbers and other sensitive information, and observe any particular requirements that apply.	
Implementation Standard	
Control Review Frequency Three (3) Years	**Assessment Frequency** Three (3) Years
Related Controls IA-4	**Reference Policy** See PT-7
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PT-07(02)	**First Amendment Information**	**P1**	**Moderate** **High**

Control Statement Systems processing, storing, or transmitting PII (to include PHI): Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.	
Discussion The Privacy Act limits agencies' ability to process information that describes how individuals exercise rights guaranteed by the First Amendment. Organizations consult with the senior agency official for privacy and legal counsel regarding these requirements.	
Implementation Standard	
Control Review Frequency Three (3) Years	**Assessment Frequency** Three (3) Years
Related Controls None;	**Reference Policy** See PT-7 Statute: Privacy Act of 1974 (P.L. 93-579); OMB Circular: A-108, A-130
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
PT-08	**Computer Matching Requirements**	**P1**	**Moderate** **High**

Control Statement Systems processing, storing, or transmitting PII (to include PHI): When a system or CMS entity (organization) processes information for the purpose of conducting a matching program:

(a) Obtain approval from the Data Integrity Board to conduct the matching program;
(b) Develop and enter into a computer matching agreement;
(c) Publish a matching notice in the Federal Register;
(d) Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and
(e) Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

Discussion

The Privacy Act establishes a set of requirements for federal and non-federal agencies when they engage in a matching program. In general, a matching program is a computerized comparison of records from two or more automated Privacy Act systems of records, or an automated system of records and automated records maintained by a non-Federal agency (or agent thereof). A matching program either pertains to Federal benefit programs or Federal personnel or payroll records. A Federal benefit match is performed for purposes of determining or verifying eligibility for payments under Federal benefit programs, or recouping payments or delinquent debts under Federal benefit programs. A matching program involves not just the matching activity itself, but also the investigative follow-up and ultimate action, if any.

CMS Businesses/Systems conducting or participating in CMAs with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records must leverage the CMS Data Integrity Board to oversee and coordinate their implementation of such matching agreements. CMS coordinates with the HHS Data Integrity Board to ensure that controls are in place to maintain both the quality and the integrity of data shared under CMAs.

The CMS Data Integrity Board ensures that sharing agreements, such as a CMA, are appropriately documented and published as required.

Implementation Standard

Control Review Frequency Three (3) Years	**Assessment Frequency** Three (3) Years

Related Controls
PM-24;
	Reference Policy
	Statute: Privacy Act of 1974 (P.L. 93-579);
	OMB Circular: A-108, A-130;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Risk Assessment

Control Number	Control Name	Priority	CMS Baseline
RA-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel and roles:
1. CMS Enterprise-level risk assessment policy that:
   a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

(c) Review and update the current risk assessment:
1. Policy within every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures within every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

Risk assessment policy and procedures address the controls in the RA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of risk assessment policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to risk assessment policy and procedures include assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

CMS provides an enterprise level risk assessment policy within the CMS IS2P2, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures).

Implementation Standard

High, Moderate & Low:

Std.1 - The CMS CIO and CISO will (a) Develop, document, and disseminate to applicable personnel and roles:
1. CMS Enterprise-level risk assessment policy that:
   a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

(c) Review and update the current risk assessment:
1. Policy within every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures within every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
PM-9, PS-8, SI-12.
(Redacted Privacy Controls: AR-2)
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-1, SM-3;
	HIPAA: 45 C.F.R. §164.308(a)(1)(i), 45 C.F.R. §164.316(a);
	NIST SP: 800-12, 800-30, 800-39, 800-100;
	OMB Circular: A-130 7.g. and 8.b.(3)(b);
	OMB Memo: M-17-12 Att. 1, A.2., M-05-08;

Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): The Privacy Office (Senior Official for Privacy) should be consulted when developing risk assessment policy and procedures to cover information systems containing PII.	
Privacy Implementation Standards Systems processing, storing, or transmitting PII (to include PHI): High & Moderate: PRIV.1 - Incorporate and monitor for changes to applicable privacy laws, regulations, and overarching policy that affect risk assessment policies to ensure the CMS and Mission/Business/System risk assessment policies remains effective. PRIV.2 - Ensure risk assessment policies support privacy to the greatest extent feasible throughout the life cycle of system collecting, using, maintaining, and/or disseminating personally identifiable information (PII).	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **RA-02**	**Control Name** **Security Categorization**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement (a) Categorize the system and information it processes, stores, and transmits; (b) Document the security categorization results, including supporting rationale, in the security plan for the system; and (c) Verify that the Authorizing Official (AO) or Authorizing Official designated representative reviews and approves the security categorization decision. Systems processing, storing, or transmitting PII (to include PHI): Involve the Senior Official for Privacy, or their designee, when conducting the security categorization process for information systems containing personally identifiable information (PII) or protected health information (PHI).			
Discussion Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in systems security engineering processes that is carried out throughout the system development life cycle. Organizations can use privacy risk assessments or privacy impact assessments to better understand the potential adverse effects on individuals. [CNSSI 1253] provides additional guidance on categorization for national security systems. Organizations conduct the security categorization process as an organization-wide activity with the direct involvement of chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, mission and business owners, and information owners or stewards. Organizations consider the potential adverse impacts to other organizations and, in accordance with [USA PATRIOT] and Homeland Security Presidential Directives, potential national-level adverse impacts.			

Security categorization processes facilitate the development of inventories of information assets and, along with CM-8, mappings to specific system components where information is processed, stored, or transmitted. The security categorization process is revisited throughout the system development life cycle to ensure that the security categories remain accurate and relevant.

All CMS systems categorized as High or Moderate are considered sensitive or contain sensitive information. All CMS systems categorized as Low are considered non-sensitive or contain non-sensitive information. Organizations implement the minimum-security requirements and controls as established in the current CMS Information Security ARS Standard, based on the system security categorization.

Implementation Standard

High, Moderate & Low:

Std. 1 - (a) Categorize the system and information it processes, stores, and transmits;

(b) Document the security categorization results, including supporting rationale, in the security/privacy plan for the system in CFACTS based on the CMS defined information types and if the systems collects PII and/or PHI; and

(c) Verify that the Authorizing Official (AO) or Authorizing Official designated representative reviews and approves the security categorization decision based on the FIPS 199 Standards for Security Categorization of Federal Information and Information Systems.

Control Review Frequency Two (2) years	**Assessment Frequency** Three (3) Years

Related Controls
CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SA-8, SC-7, SC-38, SI-12.
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FIPS: 199, 200;
	FISCAM: AS-1, SM-2;
	HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(A), 45 C.F.R. §164.308(a)(1)(ii)(B), 45 C.F.R. §164.308(a)(7)(ii)(E);
	NIST SP: 800-30, 800-37, 800-39, 800-60 v1, 800-60 v2, 800-160 v1;
	OMB Memo: M-17-12 Att. 1, A.2, M-06-16, M-14-04;
	CNSSI 1253.

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

(a) The organization should apply the “high water mark” concept to their HVA systems by properly categorizing HVAs and at least no lower than a Moderate based on the definition of the impacts defined in FIPS 199.

(b) Document the security categorization results, including supporting rationale, in the security plan for the system; and

(c) Verify that the Authorizing Official (AO) or Authorizing Official designated representative reviews and approves the security categorization decision.

HVA Discussion

Clearly defined HVA system boundaries are a prerequisite for security categorization decisions. Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are comprised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in the systems security engineering processes carried out throughout the system development life cycle.

HVA Implementation Standard

Control Number RA-03	**Control Name** Risk Assessment	**Priority** P1	**CMS Baseline** Low Moderate High

Control Statement

(a) Conduct a risk assessment, including:

1. Identifying threats to and vulnerabilities in the system;

2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

(b) Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

(c) Document risk assessment results in the applicable security and privacy plans and risk assessment report;

(d) Review risk assessment results within every 365 days;

(e) Disseminate risk assessment results to designated affected stakeholders, Business Owners(s), and the CMS CISO; and

(f) Update the risk assessment report before issuing a new Authority to Operate (ATO)/authorization or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system or if none of these events occur, update at a minimum every three (3) years.

Discussion

Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.

Organizations can conduct risk assessments at all three levels in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any stage in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including preparation, categorization, control selection, control implementation, control assessment, authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development life cycle.

Risk assessments can also address information related to the system, including system design, the intended use of the system, testing results, and supply chain-related information or artifacts. Risk assessments can play an important role in control selection processes, particularly during the application of tailoring guidance and in the earliest phases of capability determination.

Implementation Standard

High, Moderate & Low:

Std. 1 - (a) Conduct a risk assessment, including:

1. Identifying threats to and vulnerabilities in the system;

2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

(b) Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

(c) Document risk assessment results in the applicable security (Information System Risk Assessment [ISRA]), and privacy plans (Privacy Impact Assessment [PIA], Third Party Web Application [TPWA] assessment {if needed}), and any additional risk assessment reports in CFACTS;

(d) Review risk assessment results within every 365 days;

(e) Disseminate risk assessment results to designated affected stakeholders, Business Owners(s), and the CMS CISO; and

(f) Update the risk assessment report before issuing a new Authority to Operate (ATO)/authorization or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system or if none of these events occur, update every three (3) years at a minimum.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
CA-3, CA-6, CM-4, CM-13, CP-6, CP-7, IA-8, MA-5, PE-3, PE-8, PE-18, PL-2, PL-10, PL-11, PM-8, PM-9, PM-28, PT-7, RA-2, RA-5, RA-7, SA-8, SA-9, SC-38, SI-12.
(Redacted Privacy Controls: AR-2)
	Reference Policy
	OMB A-130;
	NIST SP: 800-30, 800-39, 800-161;
	IR 8023, IR 8062, IR 8272.

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

A standardized risk assessment process should include a consideration of risks associated with the collection, maintenance, and use of sensitive information such as PII. Effective implementation of privacy risk management processes requires both organizational and information system processes across the life cycle of the mission, business processes, and information system. An evaluation of privacy risk for an information system benefits an organization and the individuals whose PII are included by enabling the organization to identify, evaluate, and manage the privacy risks for the information in that system. The content of the privacy risk assessment performed under this control should be addressed in concert with the privacy risk evaluation conducted through the internal risk management process to ensure privacy risks are identified, evaluated, and managed in information systems containing privacy-related sensitive information.

A standardized risk assessment process should include a consideration of risks associated with the collection, maintenance, and use of sensitive information such as PII. An evaluation of risks associated with the potential impact of loss of the PII must be identified within the overall risk assessment. All risk assessment documentation must reflect these findings. Effective implementation of privacy risk management processes requires both organizational and information system processes across the life cycle of the mission, business processes, and information system. An evaluation of privacy risk for an information system benefits an organization and the individuals whose PII are included by enabling the organization to identify, evaluate, and manage the privacy risks for the information in that system. The content of the privacy risk assessment performed under this control should be addressed in concert with the privacy risk evaluation conducted through the internal risk management process to ensure privacy risks are identified, evaluated, and managed in information systems containing privacy-related sensitive information.

Discussion for systems processing, storing, or transmitting PHI:

The Department of Health and Human Services has issued Final Guidance on Risk Analysis (Assessment) under the HIPAA Security Rule. The Guidance on Risk Analysis Requirements under the HIPAA Security Rule (HYPERLINK ""http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf"".) provides additional information and guidance.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Include an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of personally identifiable information (PII) in the related risk assessment documentation.

PRIV.2 - Document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII;

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Document risk assessment results in a HIPAA Risk Analysis, and associated risks to PHI must be identified within the overall risk assessment. All risk assessment documentation must reflect these findings.

PRIV.2 - All HIPAA Risk Analysis documentation must be maintained for 6 years from the date of creation or date it was last in effect – whichever is later.

HVA Control Statement

The organization should:

a. conduct a risk assessment, including: the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information, and the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. integrate risk assessment results and risk management decisions from the organization and mission or business process erspectives with system-level risk assessments;

c. document risk assessment results in the HVA system security plan, HVA risk assessment report, or other agency-defined HVA risk assessment document;

d. review risk assessment results at least biannually;

e. disseminate risk assessment results to the HVA system owners and staff; and

f. update the risk assessment at least annually or when there are significant changes to the information system or environment of operation (including identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

HVA Discussion

Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of systems. Risk assessments also consider risk from external parties, including individuals accessing organizational systems; contractors operating systems on behalf of the organization; service providers; and outsourcing entities.

HVA Implementation Standard

Control Number **RA-03(01)**	**Control Name** **Supply Chain Risk Assessment**	**Priority**	**CMS Baseline** **Low** **Moderate** **High** **HVA**

Control Statement (a) Assess supply chain risks associated with systems, system components, and system services in accordance with HHS Policy for Cyber Supply Chain Risk Management; and (b) Update the supply chain risk assessment plan annually and/or when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.
Discussion Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.
Implementation Standard High, Moderate & Low: Std.1 – (a) Assess supply chain risks associated with systems, system components, and system services in accordance with HHS Policy for Cyber Supply Chain Risk Management; and (b) Update the supply chain risk assessment plan annually and/or when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain; and (c) Publish the supply chain risk assessment plan within CFACTS.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls RA-2, RA-9, PM-17, PM-30, SR-2	**Reference Policy**

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement (a) assess supply chain risks associated with the HVA, HVA components, and HVA system services; and (b) Review and update the supply chain risk assessment at least annually, when there are significant changes to the relevant supply chain, or when changes to the HVA, environments of operation, or other conditions may necessitate a change in the supply chain.
HVA Discussion Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.
HVA Implementation Standard

Control Number **RA-05**	**Control Name** **Vulnerability Monitoring and Scanning**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**

Control Statement

(a) Monitor and scan for vulnerabilities in the system and hosted applications no less often than once every 72 hours and when new vulnerabilities potentially affecting the system are identified and reported;

(b) Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;
4. Complying with DHS Continuous Diagnostics and Mitigation program and CMS requirements; and
5. Complying with required reporting metrics (e.g., CyberScope).

(c) Analyze vulnerability scan reports and results from vulnerability monitoring and control assessments;

(d) Remediate legitimate vulnerabilities based on the Business Owner’s risk prioritization in accordance with the guidance defined under security control SI-02;

(e) Share information obtained from the vulnerability monitoring process and control assessments with designated/affected stakeholders, personnel, or roles on a “need to know” basis to help eliminate similar vulnerabilities in other systems (i.e., systemic weaknesses or deficiencies); and

(f) Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Discussion

Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability monitoring (including scans). Organizations determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities such as infrastructure components (e.g., switches, routers, guards, sensors), networked printers, scanners, and copiers are not overlooked. The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced, and as new scanning methods are developed, helps to ensure that new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability monitoring and analyses for custom software may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools, including web-based application scanners, static analysis tools, and binary analyzers.

Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. Vulnerability monitoring may also include continuous vulnerability monitoring tools that use instrumentation to continuously analyze components. Instrumentation-based tools may improve accuracy and may be run throughout an organization without scanning.

Vulnerability monitoring tools that facilitate interoperability include tools that are Security Content Automated Protocol (SCAP) validated. Thus, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments such as red team exercises provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Vulnerability monitoring also includes a channel and process for receiving reports of security vulnerabilities from the public at-large. Vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports, including notification authorizing good-faith research and disclosure of security vulnerabilities. Organizations generally expect that such research is happening with or without their authorization, and can use public vulnerability disclosure channels to increase the likelihood that discovered vulnerabilities are reported directly to the organization for remediation.

Organizations may also employ the use of financial incentives (also known as “bug bounties”) to further encourage external security researchers to report discovered vulnerabilities. Bug bounty programs can be tailored to the organization’s needs. Bounties can be operated indefinitely or over a defined period of time, and can be offered to the general public or to a curated group. Organizations may run public and private bounties simultaneously, and could choose to offer partially credentialed access to certain participants in order to evaluate security vulnerabilities from privileged vantage points.

The organization remediates vulnerabilities based on the Business Owner’s risk prioritization in accordance with the guidance defined under SI-02. Penetration testing is covered under CA-08. Contact your CRA or the CCIC for the list of compliant formats.

Implementation Standard

High, Moderate & Low:

Std.1 - Vulnerability scans must be performed when new vulnerabilities, risks, or threats potentially affecting the system/applications are identified and reported or upon request from CMS.

Std.2 - Vulnerability scanning tools results must be searchable by the CCIC:

(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Vulnerability scan information sources include systems, appliances, devices, services, and applications (including databases); and
(c) CCIC directed vulnerability scan information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.3 - As required by CMS, raw results from vulnerability scanning tools must be available in an unaltered format to the CCIC.
Std.4 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational monitoring status and security posture information.

Control Review Frequency Seventy-Two (72) Hours	**Assessment Frequency** Monthly

Related Controls
CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11.
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, AS-3, CM-5, SM-5;
	HSPD: HSPD 7 F(19), G(24);
	NIST SP: 800-37, 800-39, 800-40, 800-53A, 800-70, 800-115, 800-126, 800-137;
	OMB Memo: M-14-03, M-16-04, M-19-03, M-20-04;
	Web: HYPERLINK "https://cwe.mitre.org/" , HYPERLINK "https://nvd.nist.gov/" ;
	ISO 29147;
	IR 7788, IR 8011-4, IR 8023

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

Systems designated as HVA:
High & Moderate:
(a) Implement vulnerability scanning capabilities to discovery and identify known flaws on HVA systems and components at least every 72 hours;
(b) Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;
4. Complying with DHS Continuous Diagnostics and Mitigation program and CMS requirements; and
5. Complying with required reporting metrics (e.g., CyberScope).

(c) Analyze vulnerability scan reports and results from vulnerability monitoring and control assessments;
(d) Remediate legitimate vulnerabilities based on the Business Owner’s risk prioritization in accordance with the guidance defined under security control SI-02;
(e) Share information obtained from the vulnerability monitoring process and control assessments with designated/affected stakeholders, personnel, or roles on a “need to know” basis to help eliminate similar vulnerabilities in other systems (i.e., systemic weaknesses or deficiencies); and
(f) Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

HVA Discussion

Per CDM requirements, organizations should implement vulnerability scanning capabilities to discovery and identify known flaws on the components at least every 72 hours. Security categorization of information and systems guide the frequency and comprehensiveness of vulnerability monitoring (including scans). Organizations should determine the required vulnerability monitoring for system components, ensuring the potential sources of vulnerabilities such as infrastructure components (e.g., switches, routers, sensors), networked printers, scanners, and copiers are not overlooked. The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced, and as new scanning methods are developed, helps to ensure new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure potential vulnerabilities in the system are identified and addressed as quickly as possible.

HVA Implementation Standard

<table>
<tr><td><b>Control Number</b>
<b>RA-05(02)</b></td><td><b>Control Name</b>
<b>Update Vulnerabilities to be Scanned</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Update the system vulnerabilities to be scanned no less often than every 72 hours, prior to a new scan, and when new vulnerabilities are identified and reported.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Due to the complexity of modern software and systems and other factors, new vulnerabilities are discovered on a regular basis. It is important that newly discovered vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High, Moderate & Low:
Std. 1 - Update the system vulnerabilities to be scanned no less often than every 72 hours, prior to a new scan, and when new vulnerabilities are identified and reported.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Monthly</td><td colspan="2"><b>Assessment Frequency</b>
Monthly</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
SI-3, SI-5</td><td colspan="2"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
HSPD: HSPD 7 F(19), G(24);
NIST SP: 800-37, 800-39, 800-137;
OMB Memo: M-14-03, M-16-04, M-19-03, M-20-04;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>RA-05(04)</b></td><td><b>Control Name</b>
<b>Discoverable Information</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Determine information about the system that is discoverable and take appropriate corrective actions to limit discoverable system information.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Discoverable information includes information that adversaries could obtain without compromising or breaching the system, for example, by collecting information the system is exposing or by conducting extensive web searches. Corrective actions include notifying appropriate organizational personnel, removing designated information, or changing the system to make the designated information less relevant or attractive to adversaries. This enhancement excludes intentionally discoverable information that may be part of a decoy capability (e.g., honeypots, honeynets, or deception nets) deployed by the organization.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High: The CCIC will:
Std. 1 - Determine information about the system that is discoverable and take appropriate corrective actions to limit discoverable system information.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
AU-13, SC-26.</td><td colspan="2"><b>Reference Policy</b>
NIST SP: 800-37, 800-39, 800-115, 800-137;
OMB Memo: M-14-03, M-16-04, M-19-03, M-20-04;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
</table>

HVA Discussion
HVA Implementation Standard

Control Number **RA-05(05)**	**Control Name** **Privileged Access**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement Implement privileged access authorization to system components, operating system, telecommunications, and configuration components for defined vulnerability scanning activities to facilitate more thorough scanning.
Discussion In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain classified or controlled unclassified information, such as personally identifiable information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning. Privileged access mechanisms must be compliant with CMS requirements for access to elevated privilege accounts. The assessment capability must support use of credentialed scans. Credentialed access is compliant with CMS policy.
Implementation Standard High & Moderate: Std.1 - Automated scanning tool functionality must be compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements to include the ability to perform credentialed scans. (a) To the extent possible, credentials will be compliant with CMS policy. Std.2 - Credentialed scanning must be performed on all information systems and network devices (including appliances). Std.3 - The organization must maintain and provide changes to the system accounts to support credentialed scanning no later than two (2) weeks prior to expiration or when other changes to the accounts are needed.

Control Review Frequency Quarterly	**Assessment Frequency** Quarterly

Related Controls
None;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-1, SM-3;
	HIPAA: 45 C.F.R. §164.308(a)(1)(i), 45 C.F.R. §164.316(a);
	NIST SP: 800-12, 800-30, 800-37, 800-39, 800-100, 800-115, 800-137;
	OMB Memo: M-14-03, M-16-04, M-19-03, M-20-04;

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **RA-05(06)**	**Control Name** **AUTOMATED TREND ANALYSES**	**Priority**	**CMS Baseline** **HVA**

Control Statement Compares the results of multiple vulnerability scans using automated mechanisms.
Discussion

<table>
<tr><td colspan="2"><b>Implementation Standard</b>
High: The CCIC will:
Std. 1 - Compare the results of multiple vulnerability scans using automated mechanisms.</td></tr>
<tr><td><b>Control Review Frequency</b>
Annually (365 Days)</td><td><b>Assessment Frequency</b>
Not Specified</td></tr>
<tr><td><b>Related Controls</b>
None;</td><td><b>Reference Policy</b></td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b>
The organization should compare the results of multiple HVA vulnerability scans using its implemented automated HVA vulnerability scanning capability.</td></tr>
<tr><td colspan="2"><b>HVA Discussion</b>
The organization can choose to compare scans from a single HVA or scans that were completed across multiple HVAs if broader trend analysis is desired. This process can help the organization correlate scanning information, as described in RA-5(10).</td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>RA-05(10)</b></td><td><b>Control Name</b>
<b>CORRELATE SCANNING INFORMATION</b></td><td><b>Priority</b></td><td><b>CMS Baseline</b>
<b>HVA</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
An attack vector is a path or means by which an adversary can gain access to a system in order to deliver malicious code or exfiltrate information. Organizations can use attack trees to show how hostile activities by adversaries interact and combine to produce adverse impacts or negative consequences to systems and organizations. Such information, together with correlated data from vulnerability scanning tools, can provide greater clarity regarding multi-vulnerability and multi-hop attack vectors. The correlation of vulnerability scanning information is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). During such transitions, some system components may inadvertently be unmanaged and create opportunities for adversary exploitation.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High: The CCIC will:
Std. 1 - Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Not Specified</td></tr>
<tr><td colspan="2"><b>Related Controls</b></td><td colspan="2"><b>Reference Policy</b></td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b>
The organization should correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors that could be used to attack the HVA.</td></tr>
<tr><td colspan="4"><b>HVA Discussion</b>
An attack vector is a path or means by which an adversary can gain access to a system in order to deliver malicious code or exfiltrate information. Organizations can use attack trees to show how hostile activities by adversaries interact and combine to produce adverse impacts or negative consequences to systems and organizations. Such information, together with correlated data from vulnerability scanning tools, can provide greater clarity regarding multi-vulnerability and multi-hop attack vectors. The correlation of vulnerability scanning information is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). During such transitions, some system components may inadvertently be unmanaged and create opportunities for adversary exploitation. Organizations can correlate both previous and current vulnerability scan results, as well as results from different HVAs that may be configured (e.g., applications, active network connects) in a similar manner.</td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>RA-05(11)</b></td><td><b>Control Name</b>
<b>Public Disclosure Program</b></td><td><b>Priority</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
The reporting channel is publicly discoverable and contains clear language authorizing good-faith research and disclosure of vulnerabilities to the organization. The organization does not condition its authorization on an expectation of indefinite non-disclosure to the public by the reporting entity, but may request a specific time period to properly remediate the vulnerability.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High, Moderate & Low:
Std. 1 - Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components via the Vulnerability Disclosure Policy Program.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Not Specified</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
None;</td><td colspan="2"><b>Reference Policy</b>
See RA-5;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>RA-07</b></td><td><b>Control Name</b>
<b>Risk Response</b></td><td><b>Priority</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Respond to findings from security and privacy assessments, monitoring, and audits in accordance with CMS risk tolerance.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Organizations have many options for responding to risk including mitigating risk by implementing new controls or strengthening existing controls; accepting risk with appropriate justification or rationale; sharing or transferring risk; or avoiding risk. The risk tolerance of the organization influences risk response decisions and actions. Risk response addresses the need to determine an appropriate response to risk before generating a plan of action and milestones entry. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so a plan of action and milestones entry is not needed. However, if the risk response is to mitigate the risk and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High, Moderate & Low:
Std. 1 - Respond to findings from security and privacy assessments, monitoring, and audits in accordance with CMS risk tolerance.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Annually (365 Days)</td><td colspan="2"><b>Assessment Frequency</b>
Not Specified</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
CA-5, IR-9, PM-4, PM-28, RA-2, RA-3, SR-2;</td><td colspan="2"><b>Reference Policy</b>
FIPS 199, FIPS 200;
NIST SP 800-30, 800-37, 800-39, 800-160 v1;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
</table>

Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **RA-08**	**Control Name** **Privacy Impact Assessments**	**Priority**	**CMS Baseline** **Moderate** **High**
Control Statement Conduct privacy impact assessments for systems, programs, or other activities before: (a) Developing or procuring information technology that processes personally identifiable information; and (b) Initiating a new collection of personally identifiable information that: 1. Will be processed using information technology; and 2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the federal government.			
Discussion A privacy impact assessment is an analysis of how personally identifiable information is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis. Organizations conduct and develop a privacy impact assessment with sufficient clarity and specificity to demonstrate that the organization fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the organization’s activity and throughout the information life cycle. In order to conduct a meaningful privacy impact assessment, the organization’s senior agency official for privacy works closely with program managers, system owners, information technology experts, security officials, counsel, and other relevant organization personnel. Moreover, a privacy impact assessment is not a time-restricted activity that is limited to a particular milestone or stage of the information system or personally identifiable information life cycles. Rather, the privacy analysis continues throughout the system and personally identifiable information life cycles. Accordingly, a privacy impact assessment is a living document that organizations update whenever changes to the information technology, changes to the organization’s practices, or other factors alter the privacy risks associated with the use of such information technology. To conduct the privacy impact assessment, organizations can use security and privacy risk assessments. Organizations may also use other related processes which may have different names, including privacy threshold analyses. A privacy impact assessment can also serve as notice to the public regarding the organization’s practices with respect to privacy. Although conducting and publishing privacy impact assessments may be required by law, organizations may develop such policies in the absence of applicable laws. For federal agencies, privacy impact assessments may be required by [EGOV]; agencies should consult with their senior agency official for privacy and legal counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision.			
Implementation Standard High, Moderate & Low: Std. 1 - Conduct privacy impact assessments for systems, programs, or other activities before: (a) Developing or procuring information technology that processes personally identifiable information; and (b) Initiating a new collection of personally identifiable information that: 1. Will be processed using information technology; and 2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the federal government.			

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Not Specified

Related Controls
CM-4, CM-9, CM-13, PT-2, PT-3, PT-5, RA-1, RA-2, RA-3, RA-7.
	Reference Policy
	Statute: E-Government Act of 2002 (P.L. 107-347);
	OMB Circular: A-130, Appendix II;

	OMB M-03-22
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
RA-09	**Criticality Analysis**		**Moderate** **High**

Control Statement

Identify critical system components and functions by performing a criticality analysis for systems, system components, or system services at decision points in the system development life cycle.

Discussion

Not all system components, functions, or services necessarily require significant protections. For example, criticality analysis is a key tenet of, for example, supply chain risk management, and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, executive orders regulations, directives, policies, and standards; system functionality requirements; system and component interfaces; and system and component dependencies. Systems engineers conduct a functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes the identification of organizational missions supported by the system; decomposition into the specific functions to perform those missions; and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities such components create. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions that are supported by the system containing the components and functions. Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early in the system development life cycle, organizations may be able to modify the system design to reduce the critical nature of these components and functions, for example, by adding redundancy or alternate paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is an important consideration. Such analysis is conducted as part of security categorization in RA-2.

Implementation Standard

High, Moderate & Low: Std. 1 - Identify critical system components and functions by performing a criticality analysis for systems, system components, or system services at decision points in the system development life cycle.

Control Review Frequency	**Assessment Frequency**
Annually (365 Days)	Annually (365 Days)
Related Controls	**Reference Policy**
CP-2, PL-2, PL-8, PL-11, PM-1, RA-2, SA-8, SA-15, SA-20, SR-5	NISTIR: 8179;

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **RA-10**	**Control Name** **Threat Hunting**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement (a) Establish and maintain a cyber threat hunting capability to: 1. Search for indicators of compromise in organizational systems; and 2. Detect, track, and disrupt threats that evade existing controls; and (b) Employ the threat hunting capability no less often than once every 72 hours.			
Discussion Threat hunting is an active means of cyber defense in contrast to the traditional protection measures such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indications of compromise include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams leverage existing threat intelligence and may create new threat intelligence, which is shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies.			
Implementation Standard Std. 1 - Respond to findings from security and privacy assessments, monitoring, and audits in accordance with CMS risk tolerance.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls CA-2, CA-7, CA-8, RA-3, RA-5, RA-6, SI-4.;		**Reference Policy** SP 800-30;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

System and Services Acquisition

Control Number	Control Name	Priority	CMS Baseline
SA-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel and roles:

1. CMS Enterprise-level system and services acquisition policy that:
   a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the system and services acquisition policy and associated controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

(c) Review and update the current system and services acquisition:

1. Policy at least every three (3) years; and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures at least every three (3)years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines

Discussion

This control addresses policy and procedures for the controls in the SA family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Restating controls does not constitute an organizational policy or procedure.

Implementation Standard

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**

PM-9; PS-8; SA-8, SI-12	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-1, SM-3;
	NIST SP: 800-12, 800-100;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
SA-02	**Allocation of Resources**	**P1**	**Low** **Moderate** **High**

Control Statement

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business planning;

b. Determine, document and allocate the resources required to protect the system or system service as part of CMS's capital planning and investment control process; and
c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

Discussion

Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain concerns throughout the system development life cycle.
Guidance for systems processing, storing, or transmitting PII (to include PHI):
Resources must be considered for the protection of privacy and confidentiality when budgeting for an information system.

Implementation Standard

Systems processing, storing, or transmitting PII (to include PHI):
As part of the capital planning and investment control process, the organization must determine, document, and allocate resources required to protect the privacy and confidentiality of personally identifiable information (PII) in the information system

Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)

Related Controls
PM-3, PM-11; PL-7; SA-9, SR-3, SR-5
	Reference Policy
	Statute: E-Government Act of 2002 (Pub. L. No. 107-347) §208;
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, AS-3, CM-3, SM-1;
	NIST SP: 800-65;
	OMB Circular: A-130 7.g. and 8.b(3)(b);
	OMB Memo: M-16-04, M-19-03;

Privacy Discussion

Guidance for systems processing, storing, or transmitting PII (to include PHI):
Resources must be considered for the protection of privacy and confidentiality when budgeting for an information system.

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):
As part of the capital planning and investment control process, the organization must determine, document, and allocate resources required to protect the privacy and confidentiality of personally identifiable information (PII) in the information system

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
SA-03	**System Development Life Cycle**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Acquire, develop, and manage the system using a formally defined and documented system development life cycle (SDLC) process that incorporates information security and privacy considerations;
b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;
c. Identify individuals having information security and privacy roles and responsibilities; and
d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

Discussion

A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational systems. The integration of security and privacy considerations early in the system development life cycle is a foundational principle of systems security engineering and privacy engineering. To apply the required controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical missions and business functions. The security engineering principles in SA-8 help individuals properly design, code, and test systems and system components.

Organizations include in system development life cycle processes, qualified personnel, including senior agency information security officers, senior agency officials for privacy, security and privacy architects, and security and privacy engineers to ensure that established security and privacy requirements are incorporated into organizational systems. Role-based security and privacy training programs can ensure that individuals having key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security and privacy requirements into enterprise architecture also helps to ensure that important security and privacy considerations are addressed throughout the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with risk management strategy of the organization. Because the system development life cycle involves multiple organizations, (e.g., external suppliers, developers, integrators, and service providers), acquisition and supply chain risk management functions and controls play a significant role in the effective management of the system during the life cycle.	
Implementation Standard High, Moderate & Low: Std.1 - The information system must be managed using: (a) The information security and privacy steps of IEEE 12207.0 standard for SDLC, as defined in the CMS Target Life Cycle (TLC), to incorporate information security and privacy control considerations; and (b) The information system architecture defined within the Technical Reference Architecture (TRA).	
Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)

Related Controls
AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-15, A-17, SA-22, SR-3, SR-5, SR-9
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-3, CM-3;
	NIST SP: 800-37, 800-64;
	OMB Circular: A-130;

Privacy Discussion Guidance for systems processing, storing, or transmitting PII (to include PHI): To ensure that privacy and security controls are appropriately considered during each phase of the SDLC, both the security and privacy offices should have a clear understanding of the requirements to protect PII. The privacy office should participate throughout the SDLC	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SA-03(01)	**MANAGE PREPRODUCTION ENVIRONMENT**		**Above Baseline**

Control Statement Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.	
Discussion	
Implementation Standard	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls	**Reference Policy**
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

<table>
<tr><td><b>Control Number</b>
SA-03(02)</td><td><b>Control Name</b>
Use of Live Operational Data</td><td><b>Priority</b></td><td><b>CMS Baseline</b>
Above Baseline</td></tr>
<tr><td colspan="4"><b>Control Statement</b>
(a) Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and
(b) Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Live data is also referred to as operational data. The use of live or operational data in preproduction (i.e., development, test, and integration) environments can result in significant risk to organizations. In addition, the use of personally identifiable information in testing, research, and training increases risk of unauthorized disclosure or misuse of such information. Thus, it is important for the organization to manage any additional risks that may result from use of live or operational data. Organizations can minimize such risk by using test or placeholder data during the design, development, and testing of systems, system components, and system services. Risk assessment techniques may be used to determine if the risk of using live or operational data is acceptable.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Not Specified</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
PM-25, RA-3;</td><td colspan="2"><b>Reference Policy</b></td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b>
To ensure that privacy and security controls are appropriately considered during each phase of the SDLC, both the security and privacy offices should have a clear understanding of the requirements to protect PII. The privacy office should participate throughout the SDLC</td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
SA-03(03)</td><td><b>Control Name</b>
TECHNOLOGY REFRESH</td><td><b>Priority</b></td><td><b>CMS Baseline</b>
Above Baseline</td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.</td></tr>
<tr><td colspan="4"><b>Discussion</b></td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Not Specified</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b></td><td colspan="2"><b>Reference Policy</b></td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
SA-04</td><td><b>Control Name</b>
Acquisition Process</td><td><b>Priority</b>
P1</td><td><b>CMS Baseline</b>
Low
Moderate
High
HVA</td></tr>
<tr><td colspan="4"><b>Control Statement</b></td></tr>
</table>

Include the following requirements, descriptions, and criteria, explicitly or by reference, using standardized contract language per the HHS Policy for Information Technology Procurements - Security And Privacy Language or CMS-Defined contract language in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;
b. Strength of mechanism requirements;
c. Security and privacy assurance requirements;
d. Controls needed to satisfy the security and privacy requirements.
e. Security and privacy documentation requirements;
f. Requirements for protecting security and privacy documentation;
g. Description of the system development environment and environment in which the system is intended to operate;
h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and
i. Acceptance criteria.

Discussion

Security and privacy functional requirements are typically derived from the high-level security and privacy requirements described in SA-2. The derived requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Assurance requirements include development processes, procedures, practices, and methodologies; and the evidence from development and assessment activities providing grounds for confidence that the required functionality is implemented and possesses the required strength of mechanism. [SP 800-160 v1] describes the process of requirements engineering as part of the system development life cycle.

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the security and privacy requirements of stakeholders. Controls are selected and implemented in order to satisfy system requirements and include developer and organizational responsibilities. Controls can include technical aspects, administrative aspects, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for controls within the system development life cycle

Security and privacy documentation requirements address all stages of the system development life cycle. Documentation provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as such criteria for any organizational acquisition or procurement.

Implementation Standard

High, Moderate & Low:

Std.1 - Contracts must include the standard CMS information security and privacy contract language.

Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)

Related Controls
CM-6, CM-8, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12, SA-15, SA-16, SA-17,SA-21, SR-3, SR-5;
(Redacted Privacy Controls: AR-7)
	Reference Policy
	Code: 5 U.S.C. §552a(m) and (e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002: (I; Pub. L. No. 107-347) §208, Federal Information Management Security Act (Pub. L. No. 107-347);
	FAR: Part 24 and 39.105;
	FedRAMP: Rev. 4 Baseline;
	FIPS: 140-2, 140-3;
	FISCAM: AS-3, CM-3;
	HIPAA: 164.314(a)(2)(i), 45 C.F.R. §164.314(a);
	NIST SP: 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137;
	OMB Circular: A-130 7.g. and Appendix 1;
	OMB Memo: M-16-04, M-19-03;
	Web: HYPERLINK "https://www.acquisition.gov/browse/index/far" , HYPERLINK "https://www.idmanagement.gov/sell/fips201/" , HYPERLINK "https://www.niap-ccevs.org/" ;

Privacy Discussion

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Contracts for information systems, components, or services must meet the privacy requirements of the Federal Government. It is much easier, and cheaper, to build privacy into a system at the acquisition phase of the life cycle than it is to bolt it on after the system is already acquired

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

When acquiring information systems, components, or services used to store, process, or transmit personally identifiable information (PII), ensure the following, in consultation with the privacy office, are included in the acquisition contract:

a. List of security and privacy controls necessary to ensure protection of PII and, if appropriate, enforce applicable privacy requirements.

b. Privacy requirements set forth in Appendix J of NIST SP 800-53, Rev. 4, including privacy training and awareness, and rules of behavior.

c. Privacy functional requirements, i.e., functional requirements specific to privacy.

d. Federal Acquisition Regulation (FAR) Clauses per FAR Part 24 (clauses 52.224-1, Privacy Act Notification, and 52.224-2, Privacy Act. and Part 39 (clauses 39.105, Privacy, and 39.116, Contract clause), and any other organization-specific privacy clauses

Systems processing, storing, or transmitting PHI:

PHI.1 - When acquiring information systems, components, or services used to store, process, or transmit PHI, in addition to the requirements for PII, ensure, in consultation with the privacy office, that any necessary memorandum of understanding, memorandum of agreement, and other data sharing agreement are obtained

HVA Control Statement

Include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;

b. Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements.

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

j. Contracts for HVA system support, services, and solutions must imply with security requirements of the Federal government and relevant organizational policies and procedures to ensure that the contractors are protecting the information and systems at the appropriate levels

HVA Discussion

All contract agreements for support or services of HVA systems or services include the relevant language from the Federal Acquisition Regulation (FAR) Section 7.103 containing information security requirements from FISMA. Contractors comply with all security requirements as defined in the contractual agreements. The organization oversees and monitors the contractor's compliance with the contract.

HVA Implementation Standard

Contract agreements for support or services of HVA systems and environment must include requirements for the application of the HVA control overlay. Contractor agreements incorporate Federal Incident Reporting Guidelines, as identified by USCERT, into Service Level Agreements

Control Number	Control Name	Priority	CMS Baseline
SA-04(01)	**Functional Properties of Controls**	**P1**	**Moderate** **High** **HVA**

Control Statement

Require the developer of the system, system component, or system service to provide a description of the functional properties of the security and privacy controls to be implemented.

Discussion Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.	
Implementation Standard	
Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)

Related Controls
SA-5;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	OMB Memo: M-16-04, M-19-03;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SA-04(02)	**Design and Implementation Information for Security Controls**	**P1**	**Moderate** **High** **HVA**

Control Statement Require the developer of the system, system component, or system service to provide design and implementation information for the security controls that includes: security-relevant external system interfaces at sufficient detail to understand the existence, purpose and use of all such interfaces; source code or hardware schematics; and high-level design documentation at sufficient detail to prove the security control implementation.	
Discussion Organizations may require different levels of detail in the documentation for the design and implementation for controls in organizational systems, system components, or system services based on mission and business requirements; requirements for resiliency and trustworthiness; and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system	
Implementation Standard	
Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)
Related Controls SA-5;	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SA-04(05)	**System, Component, and Service Configurations**		**High** **HVA**

Control Statement Require the developer of the system, system component, or system service to:

(a) Deliver the system, component, or service with organizationally defined security configurations implemented; and (b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.	
Discussion Examples of security configurations include the U.S. Government Configuration Baseline (USGCB), Security Technical Implementation Guides (STIGs), and any limitations on functions, ports, protocols, and services. Security characteristics can include requiring that default passwords have been changed.	
Implementation Standard	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls CM-8	**Reference Policy** See SA-5;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
SA-04(09)	**Functions, Ports, Protocols, and Services in Use**	**P1**	**Moderate** **High**

Control Statement Require the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	
Discussion The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design stages) allows organizations to influence the design of the system, system component, or system service. This early involvement in the system development life cycle helps organizations avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or requiring system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-9 describes the requirements for external system services. Organizations identify which functions, ports, protocols, and services are provided from external sources.	
Implementation Standard	
Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)

Related Controls
CM-7, SA-9;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	OMB Memo: M-16-04, M-19-03;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
SA-04(10)	**Use of Approved PIV Products**	**P1**	**Low** **Moderate** **High**

Control Statement Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.	
Discussion Products on the FIPS 201-approved products list meet NIST requirements for Personal Identity Verification (PIV) of Federal Employees and Contractors. PIV cards are used for multifactor authentication in systems and organizations.	
Implementation Standard	
Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)
Related Controls IA-2, IA-8, PM-9	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SA-05	**System Documentation**	**P2**	**Low** **Moderate** **High** **HVA**

Control Statement a. Obtain or develop administrator documentation for the system, system component, or system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security and privacy functions and mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative or privileged functions; b. Obtain or develop user documentation for the system, system component, or system service that describes: 1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and 3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals; c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and evaluate whether such documentation is essential for the effective implementation or operation of security controls in response; and d. Distribute documentation to defined personnel or roles (defined in the applicable system security plan [SSP])	
Discussion System documentation helps personnel understand the implementation and the operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used, for example, to support the management of supply chain risk, incident response, and other functions. Personnel or roles requiring documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system. Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation.	
Implementation Standard	
Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)
Related Controls	**Reference Policy** FedRAMP: Rev. 4 Baseline;

CM4, CM-7, CM-6, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3, PS-2	FISCAM: AS-3, AS-5, CM-2, CP-2;
	OMB Memo: M-16-04, M-19-03;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SA-08**	**Control Name** **Security and Privacy Engineering Principles**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement Apply information security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components. a. Per NIST SP 800-160 Vol.1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems and NIST SP-800, Vol. 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach. b. CMS-defined systems security and privacy engineering principles. c. Apply secure coding per the HHS Policy for Software Development Secure Coding Practices.			
Discussion Systems security and privacy engineering principles are closely related to and are implemented throughout the system development life cycle (see SA-3). Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For existing systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security and privacy engineering principles help organizations develop trustworthy, secure, and resilient systems and reduce the susceptibility to disruptions, hazards, threats, and creating privacy problems for individuals. Examples of system security engineering principles include: developing layered protections; establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring controls to meet organizational needs; performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply systems security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and services; reduce risk to acceptable levels; and make informed risk management decisions. System security engineering principles can also be used to protect against certain supply chain risks including incorporating tamper-resistant hardware into a design.			
Implementation Standard High & Moderate: Std.1 - The information system must follow system security and privacy engineering principles consistent with: (a) The information security steps of the CMS Target Life Cycle (TLC) to incorporate information security and privacy control considerations; (b) The information system architecture defined within the Technical Reference Architecture (TRA); and (c) The Technical Review Board (TRB) processes defined by CMS.			

Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)

Related Controls
PL-8, PM-7, RA-2, RA-9, SA-3, SA-4, SA-15, SA-17, SA-20, SC-2, SC-3, SC-32, SC-39, SR-2, SR-3, SR-5, AR-7
(Redacted Privacy Controls: AR-7)
	Reference Policy
	Statute: E-Government Act of 2002 (Pub. L. 107-347) §208;
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-3, CM-3;
	NIST SP: 800-27;

<table>
<tr><td></td><td>OMB Circular: A-130 7.g.;
OMB Memo: M-05-08, M-03-22, M-16-04, M-19-03;</td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b>
Guidance for systems processing, storing, or transmitting PII (to include PHI):
When applying information system security engineering principles in the specification, design, development, implementation, and modification of an information system containing personally identifiable information (PII), the organization should also apply privacy-enhanced system design and development principles described in this control.</td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b>
High & Moderate:
Std.1 - The information system must follow system security engineering principles consistent with:
(a) The information security steps of the CMS Target Life Cycle (TLC) to incorporate information security control considerations;
(b) The information system architecture defined within the Technical Reference Architecture (TRA); and
(c) The Technical Review Board (TRB) processes defined by CMS.</td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="2"><b>HVA Discussion</b></td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>SA-08(33)</b></td><td><b>Control Name</b>
<b>MINIMIZATION</b></td><td><b>Priority</b></td><td><b>CMS Baseline</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Implement the privacy principle of minimization using techniques defined by the CMS Privacy Office.</td></tr>
<tr><td colspan="4"><b>Discussion</b></td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Not Specified</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b></td><td colspan="2"><b>Reference Policy</b>
PE-8, PM-25, SC-42, SI-12.</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>SA-09</b></td><td><b>Control Name</b>
<b>External System Services</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b>
<b>HVA</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
a. Require that providers of external system services comply with organizational security and privacy requirements and employ appropriate controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Define and document organizational oversight and user roles and responsibilities regarding external information system services in an SLA or similar agreement; and</td></tr>
</table>

c. Employs defined processes, methods, and techniques (defined in the applicable security plan [SSP]) to monitor security control compliance by external service providers on an ongoing basis.

Discussion

External system services are services that are provided by an external provider and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a certain level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on relationships between organizations and the external providers. Organizations document the basis for the trust relationships so the relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

Implementation Standard

Systems processing, storing, or transmitting PHI:

PHI.1 - A covered entity or business associate under HIPAA or HITECH may create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations.

Control Review Frequency	**Assessment Frequency**
Monthly	Annually (365 Days)

Related Controls	**Reference Policy**

AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR-5	FedRAMP: Rev. 4 Baseline;
	HIPAA: 45 C.F.R. §164.530, 45 C.F.R. §164.308(b)(1), 45 C.F.R. §164.308(b)(4), 45 C.F.R. §164.314(a)(1), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(ii);
	HSPD: HSPD 7 D(8);
	NIST SP: 800-35;
	OMB Memo: M-16-04, M-19-03;

Privacy Discussion

Discussion for systems processing, storing, or transmitting PII (to include PHI):

Contracts and other acquisition-related documents provide an enforceable means to ensure privacy and security controls are provided for PII shared with or disclosed to recipients outside of the organization, such that contractors and service providers protect PII in the same way the organization does.

Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Official for Privacy (SOP), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control.

Systems processing, storing, and transmitting PHI:

The information security requirements and controls are documented through a written contract, or other arrangement that meets the requirements of 45 C.F.R. §164.314(a). This guidance is not intended to cover the acquisition of services of all third-party providers, only those who rise to the level of a business associate of a covered entity

Privacy Implementation Standards

Systems processing, storing, or transmitting PHI:

PHI.1 - A covered entity or business associate under HIPAA or HITECH may create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations.

PHI.2 - Under HIPAA, a business associate must ensure external service contracts, or other arrangements with subcontractors, meet the requirements of 45 §C.F.R. §164.504€

HVA Control Statement

a. Require providers of external services comply with organizational security and privacy requirements and comply with the specifications defined in the HVA control overlay.;

b. Define and document organizational oversight and user roles and responsibilities regarding external information system services in an SLA or similar agreement; and

c. Employs defined processes, methods, and techniques (defined in the applicable security plan [SSP]) to monitor security control compliance by external service providers on an ongoing basis.

HVA Discussion

External system services are services that are provided by an external provider and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. Organizations should establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. Organizations should document the basis for the trust relationships so the relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements.
HVA Implementation Standard

Control Number **SA-09(01)**	**Control Name** **RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS**	**Priority**	**CMS Baseline** **Moderate** **High** **HVA**
Control Statement (a) Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and (b) Verify that the acquisition or outsourcing of dedicated information security services is approved by MAC-defined personnel or roles].			
Discussion			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls CA-6, RA-3, RA-8.		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SA-09(05)**	**Control Name** **Processing, Storage, and Service Location**	**Priority** **P3**	**CMS Baseline** **Above Baseline**
Control Statement Restrict the location of information processing; information or data; system services to organization defined locations based on program requirements or conditions.			
Discussion The location of information processing, information and data storage, or system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions and business functions. The impact occurs when external providers control the location of processing, storage, or services. The criteria that external providers use for the selection of processing, storage, or service locations may be different from the criteria organizations use. For example, organizations may desire that data or information storage locations are restricted to certain locations to help facilitate incident response activities in case of information security or privacy incidents. Incident response activities including forensic analyses and after-the-fact investigations, may be adversely affected by the governing laws, policies, or protocols in the locations where processing and storage occur and/or the locations from which system services emanate.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls SA-5, SR-4		**Reference Policy** FedRAMP: Rev. 4 Baseline; OMB Circular: A-130 7.g. 9.b and 9.c.;	
Privacy Discussion The location of information processing, information/data storage, or information system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. The			

criteria external providers use for the selection of processing, storage, or service locations may be different from organizational criteria. For example, organizations may want to ensure that data/information storage locations are restricted to certain locations to facilitate incident response activities (e.g., forensic analyses, after-the-fact investigations) in case of information security breaches/compromises. Such incident response activities may be adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which information system services emanate. Other countries have different requirements for the protection of PII of either their own citizens or for transfer of PII across national borders. When selecting a service provider, the location for storage, maintenance, or processing must be considered. Some organizations, such as European Union member states, have very stringent data transfer restriction requirements and your organization may have a treaty or other agreement for data exchange and/or protection. Consult with your legal counsel or your organization's liaison to the Department of State
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **SA-10**	**Control Name** **Developer Configuration Management**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement Require the developer of the system, system component, or system service to: a. Perform configuration management during system, component, or service: design; development; implementation; and operation.; b. Document, manage, and control the integrity of changes to configuration items under configuration management. c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to defined personnel or roles (defined in the applicable systems security plan [SSP])
Discussion Organizations consider the quality and completeness of configuration management activities conducted by developers as direct evidence of applying effective security controls. Controls include protecting from unauthorized modification or destruction, the main copies of material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and to prevent unauthorized changes. The configuration items that are placed under configuration management include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation. Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance stage of the system development life cycle
Implementation Standard

Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)

Related Controls
CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SA-12, SI-2, SR-3, SR-4, SR-5, SR-6
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-3, CM-3;
	NIST SP: 800-128;
	OMB Memo: M-16-04, M-19-03;

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion

Control Number	Control Name	Priority	CMS Baseline
SA-11	**Developer Testing and Evaluation**	**P2**	**Moderate** **High** **HVA**

Control Statement

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:
a. Develop and implement a plan for ongoing security and privacy assessments;
b. Perform unit; integration; system; and regression testing/evaluation in accordance with the CMS Target Life Cycle (TLC);
c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during testing and evaluation.

Discussion

Developmental testing and evaluation confirms that the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. The interconnections or changes, including upgrading or replacing applications, operating systems, and firmware, may adversely affect previously implemented controls. Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as manual code review; security architecture review; penetration testing; and static analysis, dynamic analysis, binary analysis, or a hybrid of the three analysis approaches.

Developers can use the analysis approaches, along with security instrumentation and fuzzing, in a variety of tools and in source code reviews. The security and privacy assessment plans include the specific activities that developers plan to carry out, including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, the frequency of the ongoing testing and evaluation, and the types of artifacts produced during those processes. The depth of testing and evaluation refers to the rigor and level of detail associated with the assessment process. The coverage of testing and evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security and privacy assessment plans, flaw remediation processes, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the system. Contracts may specify protection requirements for documentation.

Implementation Standard

High & Moderate
Std.1 - If the security control assessment results are used in support of the security authorization process for the information system, ensure that no security relevant modifications of the information systems have been made after the assessment and after selective verification of the results.
Std.2 - Use hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.
Std.3 - All systems supporting development and pre-production testing are connected to an isolated network separated from production systems. Network traffic into and out of the development and pre-production testing environment is only permitted to facilitate system testing, and is restricted by source and destination access control lists (ACLs) as well as ports and protocols.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Annually (365 Days)
Related Controls	**Reference Policy**

CA-2, CM-4, SA-3, SA-4, SA-5, SI-2;
(Redacted Privacy Controls: AR-7)
	Code: 5 U.S.C. §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) §208, and Title III;
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-3, CM-3;
	ISO/IEC: 15408;

	OMB Circular: A-130 7.g.; OMB Memo: M-03-22; Web: HYPERLINK "https://capec.mitre.org/" , HYPERLINK "https://cve.mitre.org/" , HYPERLINK "https://cwe.mitre.org/" , HYPERLINK "https://nvd.nist.gov/" ;
Privacy Discussion	
Privacy Implementation Standards Systems processing, storing, or transmitting PII (to include PHI): For information systems containing PII, the organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan that includes assessment of privacy controls. b. Conduct tests that: 1. Minimize to the use of PII to the maximum extent practicable; 2. Use actual PII only if a formal memorandum of agreement (MOA), memorandum of understanding (MOU), or data exchange agreement has been established between the data owner of the PII and the entity developing/testing the information system including how loss, theft, or compromise (i.e., breach) of PII is to be handled; 3. Use de-identified or anonymized PII to the maximum extent practicable; and 4. Coordinate use of PII with the privacy office before conducting any testing.	
HVA Control Statement Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to: a. Develop and implement a plan for ongoing security and privacy assessments; b. Perform unit; integration; system; and regression testing/evaluation in accordance with the CMS Target Life Cycle (TLC); c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during testing and evaluation. f. Include contract language requiring developers to create and document security and privacy test plans and test all security and privacy controls during development, including the HVA overlay controls.	
HVA Discussion Developmental testing and evaluation can confirm the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. The interconnections or changes, including upgrading or replacing applications, operating systems, and firmware, may adversely affect previously implemented controls. Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws.	
HVA Implementation Standard	

Control Number **SA-11(01)**	**Control Name** **STATIC CODE ANALYSIS**	**Priority**	**CMS Baseline** **HVA**
Control Statement Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.			
Discussion			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	
Related Controls		**Reference Policy**	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			

The organization should ensure static code analysis is performed on applications to identify code weaknesses and outdated or vulnerable libraries as part of the development lifecycle. Contractual language for contractor development requires the contractor to perform this task as part of the deliverables. Organizations should also require static code analysis for all modifications, updates, or additions to applications or systems prior to implementation.
HVA Discussion Static code analysis provides a technology and methodology for security reviews and includes checking for weaknesses in the code and checking for incorporation of libraries or other included code with known vulnerabilities or that are out-of-date and not supported. Static code analysis can be used to identify vulnerabilities and to enforce secure coding practices and is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static code analysis can provide clear remediation guidance along with defects to enable developers to fix such defects.
HVA Implementation Standard

Control Number **SA-11(05)**	**Control Name** **Penetration Testing**	**Priority** **P3**	**CMS Baseline** **Above Baseline**
Control Statement Require the developer of the system, system component, or system service to perform penetration testing: (a)In a manner that is no less stringent than required under CA-8; and (b)prior to system deployment in the production environment.			
Discussion			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	

Related Controls
CA-8;
		Reference Policy
		Code: 5 U.S.C. §552a(b) and (e)(10);
		Statute: Privacy Act of 1974 (P.L. 93-579);
		NIST SP: 800-115;
		General Accounting Office (GAO);
		OMB Circular: A-130 7.g. and 8.b.(2)(c)(iii);	

Privacy Discussion			
Privacy Implementation Standards Systems processing, storing, or transmitting PII (to include PHI): If the system contains personally identifiable information (PII), then the penetration testing requirements of CA-8, as specified above in this overlay, must be applied.			
HVA Control Statement The organization should require developers of applications or components to perform penetration test, prior to implementation, against new and updates, upgrades, or changes to applications or components as part of the contractual requirements. Organizations should define policy and processes around expediting critical patches as necessary based on risk assessments. The purpose of penetration testing is to identify potential vulnerabilities in solution resulting from development errors, configuration faults, or other operational weaknesses or deficiencies. Penetration testing is often performed in conjunction with automated and manual code reviews to provide greater levels of analysis. Organizations should monitor and track contractor compliance with contractual requirements.			
HVA Discussion Penetration testing is an assessment methodology in which assessors, using all available information technology product or system documentation and working under specific constraints, attempt to circumvent implemented security and privacy features of information technology products and systems. The objective of penetration testing is to discover vulnerabilities in systems, system components and services resulting from implementation errors, configuration faults, or other operational weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible.			
HVA Implementation Standard Ensure testing of new or modified application or components prior to implementation to protect against possible loss of confidentiality, integrity, and availability.			

Control Number **SA-11(08)**	**Control Name** **Dynamic Code Analysis**	**Priority** **P3**	**CMS Baseline** **Above Baseline**
Control Statement The organization requires information systems, system components, and information system services to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.			
Discussion Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to ensure that security functionality performs in the way it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies derive from the intended use of applications and the associated functional and design specifications for the applications. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis (checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (checking for words that are out of place in software code such as non-English language words or derogatory terms).			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	

Related Controls
None;
		Reference Policy
		FedRAMP: Rev. 4 Baseline;
		OMB Memo: M-14-03, M-16-04, M-19-03, M-20-04;	

Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement The organization should require developers of applications or components to perform dynamic code analysis during the system development lifecycle and prior to implementation as part of organizational policies and contractual agreements. Dynamic code analysis typically leverages automated tools to test security functionality to verify the effectiveness of the security. An example includes fuzz testing which induces intentional program failures by using malformed or random data injection into software programs. Organizations should monitor and track contractor compliance with organizational policies and contractual requirements.			
HVA Discussion Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to ensure that security functionality performs in the way it was designed. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis and/or concordance analysis.			
HVA Implementation Standard Review and analyze code dynamically to detect flaws, vulnerabilities, or code defects to protect against possible loss of confidentiality, integrity, and availability.			

Control Number **SA-15**	**Control Name** **Development Process, Standards, and Tools**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**
Control Statement a. Require the developer of the system, system component, or system service to follow a documented development process that: 1.Explicitly addresses security and privacy requirements; 2.Identifies the standards and tools used in the development process; 3.Documents the specific tool options and tool configurations used in the development process; and 4.Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and			

b. Review the development process, standards, tools, tool options, and tool configurations at least every three (3) years to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all applicable System Acquisition (SA) and Configuration Management (CM) security controls.	
Discussion Development tools include programming languages and computer-aided design systems. Reviews of development processes include the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and to prevent unauthorized changes	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls SA-3, SA-8; MA-6, SA-4, SA-8, SA-10, SA-11, SR-3, SR-4, SR-5, SR-6, SR-9	**Reference Policy** OMB Memo: M-16-04, M-19-03;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SA-15(03)**	**Control Name** **Criticality Analysis**	**Priority**	**CMS Baseline** **Moderate** **High** **HVA**
Control Statement Require the developer of the system, system component, or system service to perform a criticality analysis throughout the system development life cycle as defined by the organization			
Discussion Criticality analysis performed by the developer provides input to the criticality analysis performed by organizations. Developer input is essential to organizational criticality analysis because organizations may not have access to detailed design documentation for system components that are developed as commercial off-the-shelf products. Such design documentation includes functional specifications, high-level designs, low-level designs, and source code and hardware schematics. Criticality analysis is important for organizational systems that are designated as high value assets. High value assets can be moderate- or high-impact systems due to heightened adversarial interest or potential adverse effects on the federal enterprise. Developer input is especially important when organizations conduct supply chain criticality analyses.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls RA-9		**Reference Policy** OMB Memo: M-16-04, M-19-03;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SA-17**	**Control Name** **Developer Security Architecture and Design**	**Priority** **P1**	**CMS Baseline** **High** **HVA**
Control Statement Require the developer of the system, system component, or system service to produce a design specification and security architecture that:			

a. Is consistent with the organization's security architecture that is an integral part the organization's enterprise architecture; b .Accurately and completely describes the required security functionality, and the allocation of controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.	
Discussion This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to help ensure that organizations develop an information security architecture, and such security architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important if/when organizations outsource the development of information systems, information system components, or information system services to external entities and there is a requirement to demonstrate consistency with the organization's enterprise architecture and information security architecture. Guidance for systems processing, storing, or transmitting PII (to include PHI): The security architecture and design identifies security and privacy controls necessary to support privacy requirements. The CMS Senior Official for Privacy is the best resource for identifying privacy requirements and privacy controls.	
Implementation Standard	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
PL-8, PM-7, SA-3, SA-8;
(Redacted Privacy Controls: AR-7)
	Reference Policy
	Code: 5 U.S.C. §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579), E-Government Act of 2002 (Pub. L. No. 107-347) Title III;
	OMB Memo: M-05-08;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SA-21	**Developer Screening**	**P3**	**Low** **Moderate** **High**
Control Statement Require that the developer of information systems, system components, or information system services: a. Has appropriate access authorizations as determined by assigned duties; and; b. Satisfies personnel screening criteria as defined by CMS.			
Discussion Developer screening is directed at external developers. Internal developer screening is addressed by PS-3. Because the system, system component, or system service may be used in critical activities essential to the national or economic security interests of the United States, organizations have a strong interest in ensuring that developers are trustworthy. The degree of trust required of developers may need to be consistent with that of the individuals accessing the systems, system components, or system services once deployed. Authorization and personnel screening criteria include clearances, background checks, citizenship, and nationality. Developer trustworthiness may also include a review and analysis of company ownership and relationships the company has with entities potentially affecting the quality and reliability of the systems, components, or services being developed. Satisfying the required access authorizations and personnel screening criteria includes providing a list of all individuals who are authorized to perform development activities on the selected system, system component, or system service so that organizations can validate that the developer has satisfied the authorization and screening requirements.			
Implementation Standard			
Control Review Frequency Annually (365 Days)		**Assessment Frequency** Three (3) Years	
Related Controls PS-3, PS-7;		**Reference Policy** Code: 5 C.F.R. §731.106;	

(Redacted Privacy Controls: AR-5)	Statute: Privacy Act of 1974 (P.L. 93-579);
	OMB Memo: M-16-04, M-19-03;
	HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(B);

Privacy Discussion Guidance for systems processing, storing, or transmitting PII (to include PHI): Access to sensitive information, such as PII and protected health information (PHI), requires both a valid need to know as documented by an access authorization request and requires a background investigation (or appropriate screening) to ensure the individual being provided access is suitable. These access authorization requirements extend to developers of information systems containing sensitive information. "Guidance for systems processing, storing, or transmitting PHI: Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization"	
Privacy Implementation Standards Systems processing, storing, or transmitting PII (to include PHI): The organization requires that the developer of systems containing personally identifiable information (PII): a. Have appropriate access authorizations as determined by the assigned contracting officer and contracting officer representative, in consultation with the organization's privacy office; and b. Satisfy organization-defined personnel screening criteria commensurate with increasing level of risk and responsibility for access to, or use of, different levels of PII.	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SA-22	**Unsupported System Components**	**P3**	**Above Baseline**
Control Statement a. Replace system components as soon as possible after discovery that support for the components is no longer available from the developer, vendor, or manufacturer, or b. Provide option(s) for alternative sources for continued support for unsupported components: provide justification and document the approval for the continued use of unsupported system components required to satisfy mission/business needs.			
Discussion Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components, for example, when vendors no longer provide critical software patches or product updates, provide an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business operations. If necessary, organizations can establish in-house support by developing customized patches for critical software components or alternatively, obtain the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include Open Source Software value-added vendors.			
Implementation Standard Std 1. Establish Plans to Mitigate or remove the unsupported system; application, operating system, COTS/GOTS software once identified Std 2. If not feasible to remove submit a waiver to the CIO for approval no less than 120 days prior to end of life; Std 3. Upgrade retire or stop the use of the unsupported element by the date specified on the support agreement by the vendor or provider.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	

Related Controls
PL-2, SA-3;
		Reference Policy
		FISCAM: AS-3, CM-2;
		HHS: End of Life Operating Systems and Applications Policy;
		NIST SP: 800-70, 800-128;	

	OMB Memo: M-07-18, M-08-22, M-16-04, M-19-03; Web: HYPERLINK "https://nvd.nist.gov/ncp/repository" , HYPERLINK "https://www.nsa.gov/" , HYPERLINK "https://nvd.nist.gov/" ;
Privacy Discussion Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

System and Communications Protection

Control Number	Control Name	Priority	CMS Baseline
SC-01	**Policy and Procedures**	**P1**	**Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel and roles:
1. CMS Enterprise-level system and communications protection policy that:
a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the system and communications protection control policy and associated system and communications protection controls;
(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the system and communications protection control policy and procedures; and
(c) Review and update the current system and communications protection:
1. Policy at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

System and communications protection policy and procedures address the controls in the SC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and communications protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and communications protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Implementation Standard

High, Moderate & Low:
Std.1 - The CIO and CISO will provide leadership and oversight to: (a) Develop, document, and disseminate to applicable stakeholder personnel via the IS2P2:
1. CMS Enterprise-level system and communications protection policy that:
a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the system and communications protection control policy and associated system and communications protection controls;
(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the system and communications protection control policy and procedures; and
(c) Review and update the current system and communications protection:
1. Policy at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Control Review Frequency	Assessment Frequency
Annually (365 days)	Three (3) Years
Related Controls	**Reference Policy**

PM-9, PS-8, SA-8, SI-12	FedRAMP: Rev.4 Baseline;
	FISCAM: AS-1, SM-1, SM-3;
	NIST SP: 800-12, 800-100;
	OMB A-130

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
SC-02	**Separation of System and User Functionality**	**P1**	**Moderate** **High**

Control Statement

Separate user functionality, including user interface services, from system management functionality.

Discussion

Application State (also known as Program State) represents the totality of everything necessary to keep your application running. System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is physical or logical. Organizations implement separation of system management functions from user functions, for example, by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. Separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles in SA-8 including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14), and SA-8(18).

Implementation Standard

Moderate & High:

Std. 1 - Separate user functionality, including user interface services, from system management functionality, i.e.., privileged user access (ADMIN type role; administer databases, network components, workstations, or servers).

Control Review Frequency	Assessment Frequency
Quarterly	Annually (365 days)
Related Controls	**Reference Policy**

AC-6,SA-4, SA-8, SC-3,SC-7, SC-32,SC-39	Code: 5 U.S.C. §552a(e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-4, AS-2;
	HIPAA: 45 C.F.R. §164.312(a)(1)
	OMB Circular: A-130 7.g. and 8.b.(3);

Privacy Discussion

Privacy Implementation Standards

Systems processing, storing, or transmitting PII (to include PHI):

In any situation where personally identifiable information (PII) is present, PII must be stored on a logical or physical partition separate from the applications and software partition.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **SC-03**	**Control Name** **Security Function Isolation**	**Priority** **P1**	**CMS Baseline** **High** **HVA**

Control Statement Isolate security functions from nonsecurity functions.
Discussion Security functions are isolated from nonsecurity functions by means of an isolation boundary implemented within a system via partitions and domains. The isolation boundary controls access to and protects the integrity of the hardware, software, and firmware that perform system security functions. Systems implement code separation in many ways, such as through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that protect the code on disk and address space protections that protect executing code. Systems can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the ideal is for all code within the defined security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions as an exception. The isolation of security functions from nonsecurity functions can be achieved by applying the systems security engineering design principles in SA-8, including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14), and SA-8(18).
Implementation Standard High: Std. 1 - Isolate security functions from nonsecurity functions.

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 days)
Related Controls AC-3, AC-6, AC-25,CM-2,CM-4, SA-4, SA-5, SA-8, SA-15, SA-17,SC-2, SC-7, SC-32,SC-39, SI-16	**Reference Policy** FISCAM: AC-4, AS-2;

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement Isolate security communications functions from nonsecurity production functions on networks to provide additional protection to security communications. For example, an external web service should only be bound to the external facing network interface and not to all interfaces on the system as there is no need for the web service to be accessible on the security communications interface.
HVA Discussion Security functions are isolated from non-security functions by means of an isolation boundary implemented via partitions and domains. The isolation boundary controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Systems implement code separation in many ways and can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the recommendation is for all code within the defined security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include non-security functions within the isolation boundary as an exception. The isolation of security functions from non-security functions can be achieved by applying the systems security engineering design principles in SA-8 including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14), and SA-8(18).
HVA Implementation Standard Std. 1 - Organizations should establish multiple network connections to isolated network and account for the potential of lateral movements through backend networks connections. Std. 2 - Organizations should configure systems to follow the principle of least functionality system in order to bind services to only the network interfaces necessary for them to function.

Control Number **SC-03(01)**	**Control Name** **Hardware Separation**	**Priority**	**CMS Baseline** **Moderate** **High**

Control Statement Employ hardware separation mechanisms to implement security function isolation.			
Discussion Hardware separation mechanisms include hardware ring architectures that are implemented within microprocessors and hardware-enforced address segmentation used to support logically distinct storage objects with separate attributes (i.e., readable, writeable)			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None.		**Reference Policy** NIST SP: 800-160;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SC-03(02)**	**Control Name** **Access and Flow Control Functions**	**Priority** **P3**	**CMS Baseline** **HVA**
Control Statement Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.			
Discussion Security function isolation occurs because of implementation. The functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include auditing, intrusion detection, and malicious code protection functions.			
Implementation Standard Moderate & High: Std. 1 - Isolate security functions from nonsecurity functions.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None;		**Reference Policy** NIST SP: 800-160;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions in order to protect the integrity of the security information of the system. The organization should implement access and flow control to and from the security functions network and other network(s) supporting the HVA environment. Organizations should ensure that multi-homed hosts do not allow lateral movement due to backend support networks through access and flow control. Examples of security functions that should be isolated using access and flow control are auditing, intrusion detection, and anti-virus functions.			
HVA Discussion Security function isolation occurs because of implementation. The functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include auditing, intrusion detection, and malicious code protection functions.			
HVA Implementation Standard			

Control Number **SC-03(03)**	**Control Name** **Minimize Nonsecurity Functionality**	**Priority** **P3**	**CMS Baseline** **Above Baseline**
Control Statement Minimize the number of nonsecurity functions included within the isolation boundary containing security functions.			
Discussion Where it is not feasible to achieve strict isolation of nonsecurity functions from security functions, it is necessary to take actions to minimize nonsecurity-relevant functions within the security function boundary. Nonsecurity functions contained within the isolation boundary are considered security-relevant because errors or malicious code in the software can directly impact the security functions of systems. The fundamental design objective is that the specific portions of systems that provide information security are of minimal size and complexity. Minimizing the number of nonsecurity functions in the security-relevant system components allows designers and implementers to focus only on those functions which are necessary to provide the desired security capability (typically access enforcement). By minimizing the nonsecurity functions within the isolation boundaries, the amount of code that is trusted to enforce security policies is significantly reduced, thus contributing to understandability.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None;		**Reference Policy** NIST SP: 800-160;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SC-04**	**Control Name** **Information in Shared System Resources**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Prevent unauthorized and unintended information transfer via shared system resources.			
Discussion Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels), where shared system resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.			
Implementation Standard High & Moderate: Std.1 - Ensure that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. Ensure that system resources shared between two (2) or more users are released back to the information system and are protected from accidental or purposeful disclosure. b. Authorize, monitor, and control the use of mobile code within the system.			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 days)	

Related Controls
AC-3, AC-4, SA-8
	Reference Policy
	Code: 5 U.S.C. §552a(b) and (e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-4, AS-2;
	HIPAA: 45 C.F.R. §164.312(a)(1);
	OMB Circular: A-130 7.g. and 8.b.(3);

Privacy Discussion	
Privacy Implementation Standards High & Moderate: Std.1 - Ensure that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. Ensure that system resources shared between two (2) or more users are released back to the information system and are protected from accidental or purposeful disclosure.	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SC-05**	**Control Name** **Denial-of-Service Protection**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement a. Protect against or limits the effects of the types of denial of service of service events defined in NIST SP 800-61, Computer Security Incident Handling Guide, and the following websites by employing defined security safeguards (defined in the applicable system security and privacy plan): - SANS Organization: "https://www.sans.org/dosstep"; - SANS Organization's Roadmap to Defeating Distributed Denial of Service (DDoS): "https://www.sans.org/dosstep/roadmap"; and - NIST National Vulnerability Database: "https://nvd.nist.gov/home" . b. Employ defined controls (defined in the applicable system security and privacy plan) by type of denial of service event to achieve the denial of service objective.			
Discussion Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a wide range of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events.			
Implementation Standard High, Moderate & Low: Std. 1 - a. Protect against or limits the effects of the types of denial of service of service events defined in NIST SP 800-61, Computer Security Incident Handling Guide, and the following websites by employing defined security safeguards (defined in the applicable system security and privacy plan): - SANS Organization: "https://www.sans.org/dosstep"; - SANS Organization's Roadmap to Defeating Distributed Denial of Service (DDoS): "https://www.sans.org/dosstep/roadmap"; and - NIST National Vulnerability Database: "https://nvd.nist.gov/home" . b. Employ defined controls (defined in the applicable system security and privacy plan) by type of denial of service event to achieve the denial of service objective.			
Control Review Frequency	**Assessment Frequency**		

Monthly	Annually (365 days)

Related Controls
CP-2, IR-4,SC-6, SC-7, SC-40
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-5, AS-2;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement a. Protect against or limits the effects of the types of denial of service attacks defined in NIST SP 800-61, Computer Security Incident Handling Guide, and the following websites by employing defined security safeguards (defined in the applicable system security and privacy plan): - SANS Organization: "https://www.sans.org/dosstep"; - SANS Organization's Roadmap to Defeating Distributed Denial of Service (DDoS): "https://www.sans.org/dosstep/roadmap"; and - NIST National Vulnerability Database: "https://nvd.nist.gov/home" . b. Employ organization-defined controls by type of denial of service event to achieve the denial of service objective. c. Implement denial of service (DoS) protection to ensure availability of the HVA and protect external facing HVAs against denial of service attacks. d. The organization should determine if the denial of service protection is to be applied at the perimeter of the HVA authorization boundary, at the perimeter of the organization's enterprise network, or both locations based on risk assessment of the potential threats to the HVA's availability.	
HVA Discussion DoS events may occur due to a variety of internal and external causes such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a variety of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial of service events. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial of service events.	
HVA Implementation Standard	

Control Number **SC-05(01)**	**Control Name** **Restrict Ability to Attack Other Systems**	**Priority**	**CMS Baseline** **HVA**
Control Statement Restrict the ability of individuals to launch types of denial-of service attacks, defined in NIST SP 800-61 as amended, against other systems.			
Discussion Restricting the ability of individuals to launch denial-of-service attacks requires the mechanisms commonly used for such attacks to be unavailable. Individuals of concern include hostile insiders or external adversaries who have breached or compromised the system and are using it to launch a denial-of-service attack. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., wired networks, wireless networks, spoofed Internet protocol packets). Organizations can also limit the ability of individuals to use excessive system resources. Protection against individuals having the ability to launch denial-of-service attacks may be implemented on specific systems or boundary devices that prohibit egress to potential target systems.			
Implementation Standard High, Moderate & Low: Std. 1 - Restrict the ability of individuals to launch types of denial-of service attacks, defined in NIST SP 800-61 as amended, against other systems.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None.		**Reference Policy** See Control SC-5.	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Restrict the ability of individuals to launch types of denial-of service attacks, defined in NIST SP 800-61 as amended, against other systems. DoS protections should be applied to the authorization boundary perimeter and at key points inside the authorization boundary to protect against loss of availability due to intentional or accidental attacks from organizational users located outside the HVA boundary.			
HVA Discussion			

Restricting the ability of individuals to launch denial of service attacks requires the mechanisms commonly used for such attacks be unavailable. Organizations should restrict the ability of individuals to connect and transmit arbitrary information on the transport medium and should limit the ability of individuals to use excessive system resources. Protection against individuals having the ability to launch denial of service attacks may be implemented on specific systems or on boundary devices prohibiting egress to potential target systems.
HVA Implementation Standard

Control Number **SC-05(02)**	**Control Name** **Capacity, Bandwidth, and Redundancy**	**Priority**	**CMS Baseline** **HVA**
Control Statement Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.			
Discussion Managing capacity ensures that sufficient capacity is available to counter flooding attacks. Managing capacity includes establishing selected usage priorities, quotas, partitioning, or load balancing.			
Implementation Standard High, Moderate & Low: Std. 1 - Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.			
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years		
Related Controls None.	**Reference Policy** See Control SC-5.		
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks and to protect against loss of availability due to lack of network resources. The organization should limit and control capacity into and out of the authorization boundary and at key points inside the boundary to ensure sufficient capacity exists to prevent network flooding DoS. Organizations should perform a risk assessment to determine the appropriate locations inside the authorization boundary based on data flow and user access.			
HVA Discussion Managing capacity ensures sufficient capacity is available to counter flooding attacks. Managing capacity includes establishing selected usage priorities, quotas, partitioning, or load balancing.			
HVA Implementation Standard			

Control Number **SC-05(03)**	**Control Name** **Detection and Monitoring**	**Priority**	**CMS Baseline** **HVA**
Control Statement (a) Employ monitoring tools defined in NIST SP 800-61 as amended or applicable system security and privacy plan to detect indicators of denial of service attacks against, or launched from, the system; and (b) Monitor system resources to determine if sufficient resources exist to prevent effective denial of service attacks.			
Discussion Organizations consider the utilization and capacity of system resources when managing risk associated with a denial of service due to malicious attacks. Denial-of-service attacks can originate from external or internal sources. System resources that are sensitive to denial of service include physical disk storage, memory, and CPU cycles. Techniques used to prevent denial-of-service attacks related to storage utilization and capacity include instituting disk quotas, configuring systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data.			

Implementation Standard High, Moderate & Low: Std. 1 - (a) Employ monitoring tools defined in NIST SP 800-61 as amended or applicable system security and privacy plan to detect indicators of denial of service attacks against, or launched from, the system; and (b) Monitor system resources to determine if sufficient resources exist to prevent effective denial of service attacks.	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls CA-7, SI-4	**Reference Policy** See Control SC-5.
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement (a) Employ inspection tools defined in NIST SP 800-61 as amended or applicable system security and privacy plan to detect indicators of denial of service anomalies both at the perimeter of the authorization boundary as well as inside the authorization boundary on access control points that form isolation zones; and (b) Monitor HVA system resources to determine if sufficient resources exist to prevent effective denial of service attacks. The organization should determine the level of inspection required for each isolation zone based on risk assessment to the HVA.	
HVA Discussion Organizations should consider utilization and capacity of system resources when managing risk from denial of service due to malicious attacks. DoS attacks can originate from external or internal sources. System resources sensitive to denial of service include physical disk storage, memory, and central processing unit cycles. Controls used to prevent denial of service attacks related to storage utilization and capacity include instituting disk quotas, configuring systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data.	
HVA Implementation Standard	

Control Number **SC-07**	**Control Name** **Boundary Protection**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement a. Monitor and control communications at the external interfaces to the system and at key internal interfaces within the system; b. Implement subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.			
Discussion Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses. [SP 800-189] provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions. Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary). Contact your CRA or the CCIC for the list of compliant formats.			
Implementation Standard High, Moderate & Low: Std.1 - Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.			

Std.2 - Utilize stateful inspection/application firewall hardware and software.
Std.3 - Utilize firewalls from two (2) or more different vendors at the various levels within the network to reduce the possibility of compromising the entire network.
Std.4 - If the system has an outward facing Web or email presence to the public internet, the organization must implement and support a technical capability to detect malware in web traffic traversing the organization’s boundary by:
(a) Monitoring assets without the need to deploy software agents (zero client footprint);
(b) Dynamically generating actionable malware intelligence;
(c) Detecting and stopping web-based and email attacks; and
(d) Sending alert data to the organization’s SIEM.
Std.5 - Aggregated boundary protection device information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include boundary protection systems, appliances, devices, services, and applications; and
(c) CCIC directed aggregated boundary protection device information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.6 - As required by CMS, raw boundary protection device information from relevant automated must be available in an unaltered format to the CCIC.

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 days)

Related Controls
AC-4, AC-17, AC-18,AC-19, AC-20,AU-13,CA-3, CM-2, CM-4,CM-7, CM-10, CP-8, IR-4, MA-4,PE-3,PL-8,PM-12 ,RA-3, SC-5, SC-26,SC-32,SC-35,SC-43
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FIPS: 199;
	FISCAM: AC-1, AS-2;
	HIPAA: 45 C.F.R. §164.312(e)(1), 45 C.F.R. §164.312(e)(2)(i);
	NIST SP: 800-41, 800-77, 800-137;

Privacy Discussion

Privacy Implementation Standards

High, Moderate & Low:
Std.1 - Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.
Std.2 - Utilize stateful inspection/application firewall hardware and software.
Std.3 - Utilize firewalls from two (2) or more different vendors at the various levels within the network to reduce the possibility of compromising the entire network.
Std.4 - If the system has an outward facing Web or email presence to the public internet, the organization must implement and support a technical capability to detect malware in web traffic traversing the organization’s boundary by:
(a) Monitoring assets without the need to deploy software agents (zero client footprint);
(b) Dynamically generating actionable malware intelligence;
(c) Detecting and stopping web-based and email attacks; and
(d) Sending alert data to the organization’s SIEM.
Std.5 - Aggregated boundary protection device information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include boundary protection systems, appliances, devices, services, and applications; and
(c) CCIC directed aggregated boundary protection device information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.6 - As required by CMS, raw boundary protection device information from relevant automated must be available in an unaltered format to the CCIC.

HVA Control Statement

a. Monitor and control communications at the external interfaces to the system and at key internal interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are physically/logically separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

HVA Discussion The organization should employ boundary protection solutions at the HVA authorization boundary to protect the information and mission critical services from adjacent systems (to include other HVAs) within the organization. HVAs that rely on supporting systems in the enterprise protected at a lower level of trust should be implemented in a manner that reduces the risk these interdependencies may introduce to the HVA. Examples of boundary protection devices include: Firewalls, Application Firewall/Proxy/Gateway (web, email, data transfers, etc.), Intrusion Detection, Service/Intrusion Prevention Services, and Application Load Balancer/Cryptographic services. Organizations should implement default deny, permit by exception for egress and ingress access control at the system boundary. All devices should be explicitly blocked (inbound and outbound) at the authorization boundary and specific access granted for communications based on source IP, destination, IP, port, and protocol. “ANY” or “ALL” rules should not be used in allow access control statements. Systems and components within the HVA environment should not have direct access to the Internet unless specifically required for the application to function. It is recommended to block Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) traffic bi-directionally for all internal systems. Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks physically or logically separated from internal networks are referred to as demilitarized zones. Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions.
HVA Implementation Standard

<table>
<tr><td><b>Control Number</b>
SC-07(03)</td><td><b>Control Name</b>
Access Points</td><td colspan="2"><b>Priority</b>
P1</td><td><b>CMS Baseline</b>
Moderate
High
HVA</td></tr>
<tr><td colspan="5"><b>Control Statement</b>
Limit the number of external network connections to the system.</td></tr>
<tr><td colspan="5"><b>Discussion</b>
Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. The Trusted Internet Connection [DHS TIC] initiative is an example of a federal guideline that requires limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.</td></tr>
<tr><td colspan="5"><b>Implementation Standard</b>
High & Moderate:
Std.1 - Implementation must route external connections via a Trusted Internet Connection (TIC) portal.</td></tr>
<tr><td colspan="3"><b>Control Review Frequency</b>
Quarterly</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 days)</td></tr>
<tr><td colspan="3"><b>Related Controls</b>
None;</td><td colspan="2"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
OMB Memo: M-19-26;</td></tr>
<tr><td colspan="5"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="5"><b>Privacy Implementation Standards</b>
High & Moderate:
Std.1 - Implementation must route external connections via a Trusted Internet Connection (TIC) portal.</td></tr>
<tr><td colspan="5"><b>HVA Control Statement</b>
Limit the number of external network connections to the HVA system in order to reduce the risk of unauthorized network access to an HVA. The organization should maintain only the minimum number of external network connections required for the HVA to function or provide a service.</td></tr>
<tr><td colspan="5"><b>HVA Discussion</b>
The Trusted Internet Connection (TIC) initiative is an example of a federal guideline requiring limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).</td></tr>
</table>

Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system. Limiting external network connections to an HVA also reduces the amount of inbound and outbound communications that must be monitored and analyzed due to fewer active data connections.

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
SC-07(04)	**External Telecommunications Services**	**P1**	**Moderate** **High**

Control Statement

(a) Implement a managed interface for each external telecommunication service;
(b) Establish a traffic flow policy for each managed interface;
(c) Protect the confidentiality and integrity of the information being transmitted across each interface;
(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;
(e) Review exceptions to the traffic flow policy within every three hundred sixty-five (365) days or implementation of major new system and remove exceptions that are no longer supported by an explicit mission or business need;
(f) Prevent unauthorized exchange of control plane traffic with external networks;
(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
(h) Filter unauthorized control plane traffic from external networks.

Discussion

External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols. See [SP 800-189] for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements.

Implementation Standard

High & Moderate:
Std. 1 - (a) Implement a managed interface for each external telecommunication service;
(b) Establish a traffic flow policy for each managed interface;
(c) Protect the confidentiality and integrity of the information being transmitted across each interface;
(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;
(e) Review exceptions to the traffic flow policy within every three hundred sixty-five (365) days or implementation of major new system and remove exceptions that are no longer supported by an explicit mission or business need;
(f) Prevent unauthorized exchange of control plane traffic with external networks;
(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
(h) Filter unauthorized control plane traffic from external networks.

Control Review Frequency	Assessment Frequency
Annually (365 days)	Annually (365 days)
Related Controls	**Reference Policy**
AC-3, SC-8	FedRAMP: Rev. 4 Baseline;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **SC-07(05)**	**Control Name** **Deny By Default — Allow By Exception**	**Priority** **P1**	**CMS Baseline** **Moderate** **High** **HVA**
Control Statement Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces and/or for specific systems.			
Discussion Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.			
Implementation Standard High & Moderate: Std. 1 - Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces and/or for specific systems.			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 days)	
Related Controls None;		**Reference Policy** FedRAMP: Rev. 4 Baseline;	
Privacy Discussion			
Privacy Implementation Standards Std.1 - Implementation must route external connections via a Trusted Internet Connection (TIC) portal.			
HVA Control Statement Deny network communications traffic to the HVA by default and allow network communications traffic by exception at managed interfaces or for authorized organization-defined HVA support systems.			
HVA Discussion Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.			
HVA Implementation Standard			

Control Number **SC-07(07)**	**Control Name** **Split Tunneling for Remote Devices**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using defined security safeguards (i.e. the use of VPN for remote connections, sufficiently provisioned with appropriate security and privacy controls).			
Discussion Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices and simultaneously, access uncontrolled networks. Split tunneling might be desirable by remote users to communicate with local system resources, such as printers or file servers. However, split tunneling can facilitate unauthorized external connections, making the system vulnerable to attack and to exfiltration of organizational information. Split tunneling can be prevented by disabling configuration settings that allow such capability in remote devices and by preventing those configuration settings from being configurable by users. Prevention can also be achieved by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments, or to a specific set of preapproved addresses, without user control. Examples of firewalls include the packet filtering firewall, circuit-level gateway, application-level gateway (aka proxy firewall), stateful inspection firewall and next-generation firewall (NGFW). Many firewall implementations incorporate features of different types of			

firewalls, so choosing a type of firewall is rarely a matter of finding one that fits neatly into any particular category. For example, an NGFW may incorporate new features, along with some of those from packet filtering firewalls, application-level gateways or stateful inspection firewalls.	
Implementation Standard High & Moderate: Std. 1 - Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using defined security safeguards (i.e. the use of VPN for remote connections, sufficiently provisioned with appropriate security and privacy controls).	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 days)
Related Controls None;	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SC-07(08)**	**Control Name** **Route Traffic to Authenticated Proxy Servers**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement Route all user-initiated internal communications traffic to untrusted external networks through authenticated proxy servers at managed interfaces.	
Discussion External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. System resources that may be requested include files, connections, web pages, or services. Client requests established through a connection to a proxy server are assessed to manage complexity and provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers that provide access to the Internet. Proxy servers can support the logging of Transmission Control Protocol sessions and the blocking of specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Note that proxy servers may inhibit the use of virtual private networks (VPNs) and create the potential for “man-in-the-middle” attacks (depending on the implementation)	
Implementation Standard High & Moderate: Std. 1 - Route all user-initiated internal communications traffic to untrusted external networks through authenticated proxy servers at managed interfaces.	
Control Review Frequency Monthly	**Assessment Frequency** Annually (365 days)
Related Controls AC-3	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SC-07(10)**	**Control Name** **Prevent Exfiltration**	**Priority**	**CMS Baseline** **HVA**
Control Statement			

(a) Prevent the exfiltration of information; and (b) Conduct exfiltration tests according to the defined frequency in the applicable system security and privacy plan.	
Discussion Prevention of exfiltration applies to both the intentional and unintentional exfiltration of information. Techniques used to prevent the exfiltration of information from systems may be implemented at internal endpoints, external boundaries, and across managed interfaces and include adherence to protocol formats, monitoring for beaconing activity from systems, disconnecting external network interfaces except when explicitly needed, employing traffic profile analysis to detect deviations from the volume and types of traffic expected, call backs to command and control centers, conducting penetration testing, monitoring for steganography, disassembling and reassembling packet headers, and using data loss and data leakage prevention tools. Devices that enforce strict adherence to protocol formats include deep packet inspection firewalls and Extensible Markup Language (XML) gateways. The devices verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices that operate at the network or transport layers. The prevention of exfiltration is similar to data loss prevention or data leakage prevention and is closely associated with cross-domain solutions and system guards that enforce information flow requirements.	
Implementation Standard High & Moderate: Std. 1 - (a) Prevent the exfiltration of information; and (b) Conduct exfiltration tests according to the defined frequency in the applicable system security and privacy plan.	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls AC-2, CA-8, SI-3	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement a. Prevent the exfiltration of information; and b. Conduct exfiltration tests according to the defined frequency in the applicable system security and privacy plan. C. Implement technical measures and enhanced inspection of traffic flow into, out of, and within the authorization boundary. Measures such as enforcing protocol validation checking, traffic monitoring, packet inspection, Secure Sockets Layer packet inspection, and beaconing traffic should be implemented on the authorization boundary devices and isolation devices throughout the environment.	
HVA Discussion This control applies to intentional and unintentional exfiltration of information. Controls to prevent exfiltration of information from systems may be implemented at internal endpoints, external boundaries, and across managed interfaces and include adherence to protocol formats, monitoring for beaconing activity from systems, disconnecting external network interfaces except when explicitly needed, employing traffic profile analysis to detect deviations from the volume and types of traffic expected or call backs to command and control centers, monitoring for steganography, disassembling and reassembling packet headers, and employing data loss and data leakage prevention tools. The various devices that enforce strict adherence to protocol formats verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SC-07(11)	**Restrict Incoming Communications Traffic**		**HVA**
Control Statement Only allow incoming communications from CMS authorized sources to be routed to CMS authorized destinations.			
Discussion General source address validation techniques are applied to restrict the use of illegal and unallocated source addresses as well as source addresses that should only be used within the system. The restriction of incoming communications traffic provides determinations that source and destination address pairs represent authorized or allowed communications. Determinations can be based on several factors, including the presence of such address pairs in the lists of authorized or allowed communications, the absence of such address pairs in lists of unauthorized or disallowed pairs, or meeting more general rules for authorized or allowed source and destination pairs. Strong authentication of network addresses is not possible without the use of explicit security protocols, and thus, addresses can often be spoofed. Further, identity-based incoming traffic restriction methods can be employed, including router access control lists and firewall rules.			

Implementation Standard High & Moderate: Std. 1 - Only allow incoming communications from CMS authorized sources to be routed to CMS authorized destinations.	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls AC-3	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Only allow incoming communications from CMS authorized sources to be routed to CMS authorized destinations. Implement incoming communications control for the HVA at the authorization boundary to limit HVA exposure to threats and reduce the attack surface of the HVA. The use of wildcards in ALLOW rules (ANY or ALL) should not be used. Default deny ANY rules with logging should be enabled.	
HVA Discussion General source address validation techniques should be applied to restrict the use of illegal and unallocated source addresses and source addresses that should only be used inside the system boundary. Restriction of incoming communications traffic provides determinations that source and destination address pairs represent authorized or allowed communications. Strong authentication of network addresses is not possible without the use of explicit security protocols and thus, addresses can often be spoofed. Also, identity-based incoming traffic restriction methods can be employed to reduce these risks.	
HVA Implementation Standard	

Control Number **SC-07(12)**	**Control Name** **Host-Based Protection**	**Priority**	**CMS Baseline** **HVA**
Control Statement Implement host-based boundary protection mechanisms at system components.			
Discussion Host-based boundary protection mechanisms include host-based firewalls. System components that employ host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.			
Implementation Standard High & Moderate: Std. 1 - Implement host-based boundary protection mechanisms at system components.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None.		**Reference Policy** FedRAMP: Rev. 4 Baseline;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Implement host-based boundary protections (e.g., firewall, Host-Based Intrusion Detection System, Host-Based Intrusion Prevention System) on the HVA system components to protect the HVA from unauthorized access or compromise as part of a defense-in-depth approach. Organizations should monitor these system activities as part of the incident monitoring processes and procedures.			
HVA Discussion Host-based boundary protection mechanisms include host-based firewalls. System components employing host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.			
HVA Implementation Standard			

Control Number **SC-07(14)**	**Control Name** **Protect Against Unauthorized Physical Connections**	**Priority** **P3**	**CMS Baseline** **HVA**
Control Statement			

Protect against unauthorized physical connections at managed interfaces.

Discussion

Systems that operate at different security categories or classification levels may share common physical and environmental controls, since the systems may share space within the same facilities. In practice, it is possible that these separate systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved by using clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls that enforce limited authorized access to these items.

Implementation Standard

High & Moderate:
Std. 1 - Protect against unauthorized physical connections at managed interfaces.

Control Review Frequency	Assessment Frequency
Not Specified	Three (3) Years

Related Controls	Reference Policy
PE-4, PE-19	HIPAA: 45 C.F.R. §164.312(e)(1), 45 C.F.R. §164.312(e)(2)(i);

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

Protect against unauthorized physical connections at managed interfaces. The organization should ensure the physical access to network components supporting HVA systems and environments are protected from unauthorized access and unauthorized connection of devices. This protection scheme is based on a risk assessment of the physical environment(s) containing HVA components.

HVA Discussion

HVA systems operating at different security categories or classification levels may share common physical and environmental controls since the systems may share space within the same facilities. In practice, it is possible that these separate systems may share common equipment. Protection against unauthorized physical connections can be achieved, for example, by using clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls enforcing limited authorized access to these items.

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
SC-07(17)	**Automated Enforcement of Protocol Formats**		**HVA**

Control Statement

Enforce adherence to protocol formats.

Discussion

System components that enforce protocol formats include deep packet inspection firewalls and XML gateways. The components verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.

Implementation Standard

High & Moderate:
Std. 1 - Enforce adherence to protocol formats.

Control Review Frequency	Assessment Frequency
Not Specified	Three (3) Years

Related Controls	Reference Policy
SC-4	FedRAMP: Rev. 4 Baseline;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

Enforce adherence to protocol formats. The organization should ensure HVA authorization boundary devices and internal boundary devices enforce protocol validation checking bi-directionally for HVA network traffic. (i.e. TCP/IP protocol validation). Nonstandard protocols are identified, addressed, and remediated following POA&M processes.

HVA Discussion

System components that enforce protocol formats include deep packet inspection firewalls and Extensible Markup Language gateways. The components verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.
HVA Implementation Standard

Control Number **SC-07(18)**	**Control Name** **Fail Secure**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.			
Discussion Fail secure is a condition achieved by employing mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces, systems do not enter into unsecure states where intended security properties no longer hold. Managed interfaces include routers, firewalls, and application gateways that reside on protected subnetworks (commonly referred to as demilitarized zones). Failures of boundary protection devices cannot lead to or cause information external to the devices to enter the devices nor can failures permit unauthorized information releases.			
Implementation Standard High: Std.1 - Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.			
Control Review Frequency Monthly		**Assessment Frequency** Annually (365 days)	
Related Controls CP-2, CP-12, SC-24		**Reference Policy** FedRAMP: Rev. 4 Baseline;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SC-07(21)**	**Control Name** **Isolation of System Components**	**Priority** **P1**	**CMS Baseline** **High** **HVA**
Control Statement Employ boundary protection mechanisms to isolate defined system components (defined in the applicable system security and privacy plan) supporting CMS missions and/or business functions.			
Discussion Organizations can isolate system components that perform different mission or business functions. Such isolation limits unauthorized information flows among system components and provides the opportunity to deploy greater levels of protection for selected system components. Isolating system components with boundary protection mechanisms provides the capability for increased protection of individual system components and to more effectively control information flows between those components. Isolating system components provides enhanced protection that limits the potential harm from hostile cyberattacks and errors. The degree of isolation varies depending upon the mechanisms chosen. Boundary protection mechanisms include routers, gateways, and firewalls that separate system components into physically separate networks or subnetworks; cross-domain devices that separate subnetworks; virtualization techniques; and the encryption of information flows among system components using distinct encryption keys.			
Implementation Standard High: Std. 1 - Employ boundary protection mechanisms to isolate defined system components (defined in the applicable system security and privacy plan) supporting CMS missions and/or business functions.			

Control Review Frequency Monthly	**Assessment Frequency** Annually (365 days)
Related Controls CA-9, SC-3	**Reference Policy** See Control SC-7;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Employ boundary protection mechanisms to isolate defined system components (defined in the applicable system security and privacy plan) supporting CMS missions and/or business functions. The organization should isolate HVA components to limit lateral movement among those components and provide the capability for increased protection of the entirety of the HVA. Additional security boundaries should be applied inside the HVA authorization boundary to isolate components requiring higher-levels of protections. Isolation examples include, enclaving off data repository systems and controlling access so that only necessary services and users can access the data store. Isolation should be established, and access controlled by boundary protection devices. Isolation can be facilitated using access control points to create multiple zones (web, application, and data zone). Organizations should also implement inspection on access control points to protect HVA data and system components. They should limit access flows outbound and inspect traffic on access control points from the enclaves to protect against exfiltration of data.	
HVA Discussion Organizations can isolate system components performing different missions or business functions. Such isolation limits unauthorized information flows among system components and provides the opportunity to deploy greater levels of protection for selected system components. Isolating system components with boundary protection mechanisms provides the capability for increased protection of individual system components and to more effectively control information flows between those components. Isolating system components provides enhanced protection that limits the potential harm from hostile cyber-attacks and errors.	
HVA Implementation Standard	

Control Number **SC-07(22)**	**Control Name** **Separate Subnets for Connecting to Different Security Domains**	**Priority**	**CMS Baseline** **HVA**
Control Statement Implement separate network addresses to connect to systems in different security domains.			
Discussion The decomposition of systems into subnetworks (i.e., subnets) helps to provide the appropriate level of protection for network connections to different security domains that contain information with different security categories or classification levels.			
Implementation Standard High & Moderate: Std. 1 - Implement separate network addresses to connect to systems in different security domains.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None.		**Reference Policy** See Control SC-7;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Implement separate network addresses to connect to systems in different security domains. The organization should implement a subnet containing its HVA and assign this subnet a separate network address to use when connecting to other HVAs or systems in different subnets or security domains.			
HVA Discussion The decomposition of systems into subnetworks (i.e., subnets) helps to provide the appropriate level of protection for network connections to different security domains containing information with different security categories or classification levels. The organization may leverage the CDM boundary protection tools and methods to aid in protecting HVA boundaries.			
HVA Implementation Standard			

Control Number **SC-07(24)**	**Control Name** **Personally Identifiable Information**	**Priority**	**CMS Baseline** **Moderate** **High**
Control Statement For systems that process personally identifiable information: (a) Apply the following processing rules to data elements of personally identifiable information: The Privacy Act of 1974. (b) Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system; (c) Document each processing exception; and (d) Review and remove exceptions that are no longer supported.			
Discussion Managing the processing of personally identifiable information is an important aspect of protecting an individual's privacy. Applying, monitoring for, and documenting exceptions to processing rules ensure that personally identifiable information is processed only in accordance with established privacy requirements.			
Implementation Standard High & Moderate: Std. 1 - For systems that process personally identifiable information: (a) Apply the following processing rules to data elements of personally identifiable information: The Privacy Act of 1974. (b) Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system; (c) Document each processing exception; and (d) Review and remove exceptions that are no longer supported.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls PT-2, SI-15		**Reference Policy** See Control SC-7;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SC-08**	**Control Name** **Transmission Confidentiality and Integrity**	**Priority** **P1**	**CMS Baseline** **Moderate** **High** **HVA**
Control Statement Protect the confidentiality and integrity of transmitted information. Any transmitted data containing sensitive information must be encrypted using a FIPS 140-2 validated module (See SC-13 and HHS Standard for Encryption of Computing Devices and Information).			
Discussion Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques.			

<table>
<tr><td colspan="2">Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls.</td></tr>
<tr><td colspan="2"><b>Implementation Standard</b>
High & Moderate:
Std. 1 - Protect the confidentiality and integrity of transmitted information. Any transmitted data containing sensitive information must be encrypted using a FIPS 140-2 validated module (See SC-13 and HHS Standard for Encryption of Computing Devices and Information).</td></tr>
<tr><td><b>Control Review Frequency</b>
Quarterly</td><td><b>Assessment Frequency</b>
Annually (365 days)</td></tr>
<tr><td><b>Related Controls</b>
AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SA-8, SC-7, SC-16, SC-20, SC-23, SC-28</td><td><b>Reference Policy</b>
[FIPS 140-3], [FIPS 197], [SP 800-52], [SP 800-77], [SP 800-81-2], [SP 800-113], [SP 800-177], [IR 8023]</td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b>
The HVA system should protect the confidentiality and integrity of transmitted information over trusted and untrusted networks (networks outside the HVA authorization boundary are not trusted). Ensure HVA information traversing a network inside and outside the HVA authorization boundary receives confidentiality and integrity protections; and any transmitted data containing sensitive information is encrypted in accordance with FIPS 140-2 validated module (See SC-13 and HHS Standard for Encryption of Computing Devices and Information).</td></tr>
<tr><td colspan="2"><b>HVA Discussion</b>
Protecting the confidentiality and integrity of transmitted information applies to internal and external networks, and any system components that can transmit information. Unprotected communication paths are exposed to the possibility of interception and modification.
Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services, may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations should determine what types of confidentiality or integrity services are available.</td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>SC-08(01)</b></td><td><b>Control Name</b>
<b>Cryptographic Protection</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPSec. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
High & Moderate:
Std. 1 - When cryptographic mechanisms are needed, the information system must use encryption products that have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2 in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Quarterly</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b></td><td colspan="2"><b>Reference Policy</b></td></tr>
</table>

SC-12, SC-13	[FIPS 140-3], [FIPS 197], [SP 800-52], [SP 800-77], [SP 800-81-2], [SP 800-113], [SP 800-177], [IR 8023]
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SC-08(02)**	**Control Name** **Pre- and Post-Transmission Handling**	**Priority** **P1**	**CMS Baseline** **Above Baseline**
Control Statement Maintain the confidentiality and integrity of information during preparation for transmission and during reception.			
Discussion Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception, including during aggregation, at protocol transformation points, and during packing and unpacking. Such unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls SC-12, SC-13		**Reference Policy** [FIPS 140-3], [FIPS 197], [SP 800-52], [SP 800-77], [SP 800-81-2], [SP 800-113], [SP 800-177], [IR 8023]	
Privacy Discussion			
Privacy Implementation Standards Because of the sensitivity of personally identifiable information (PII) and protected health information (PHI), the confidentiality and integrity of such information in transit must be assured. Systems processing, storing, or transmitting PII (to include PHI): FIPS-validated encryption or protected distribution systems are used to protect personally identifiable information (PII) to ensure the information's confidentiality and integrity during transmission.			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SC-8(03)**	**Control Name** **Cryptographic Protection for Message Externals**	**Priority**	**CMS Baseline** **Above Baseline**
Control Statement Implement cryptographic mechanisms to protect message externals unless otherwise protected by alternative physical controls defined in applicable system security and privacy plan.			
Discussion Cryptographic protection for message externals addresses protection from the unauthorized disclosure of information. Message externals include message headers and routing information. Cryptographic protection prevents the exploitation of message externals and applies to internal and external networks or links that may be visible to individuals who are not authorized users. Header and routing information is sometimes transmitted in clear text (i.e., unencrypted) because the information is not identified by organizations as having significant value or because encrypting the information can result in lower network performance or higher costs. Alternative physical controls include protected distribution systems.			
Implementation Standard			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	

Related Controls SC-12, SC-13	**Reference Policy** [FIPS 140-3], [FIPS 197], [SP 800-52], [SP 800-77], [SP 800-81-2], [SP 800-113], [SP 800-177], [IR 8023]
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
SC-10	**Network Disconnect**	**P2**	**Moderate** **High**
Control Statement a. Terminate the network connection associated with a communications session at the end of the session or: 1. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and 2. Forcibly disconnects inactive VPN connections after thirty (30) minutes or less of inactivity; and b. Terminate or suspend network connections (i.e., a system to system interconnection) upon issuance of an order by the CMS CIO, CISO, or Senior Official for Privacy (SOP).			
Discussion Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses. A session is an encounter between an end-user interface device (e.g., computer, terminal, process) and an application, including a network logon—the AC-11 session lock applies. A connection-based session is one that requires a connection to be established between hosts prior to an exchange of data.			
Implementation Standard High & Moderate: Std. 1 - a. Terminate the network connection associated with a communications session at the end of the session or: 1. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and 2. Forcibly disconnects inactive VPN connections after thirty (30) minutes or less of inactivity; and b. Terminate or suspend network connections (i.e., a system to system interconnection) upon issuance of an order by the CMS CIO, CISO, or Senior Official for Privacy (SOP).			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 days)	
Related Controls AC-17, SC-23		**Reference Policy** None.	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number	Control Name	Priority	CMS Baseline
SC-12	**Cryptographic Key Establishment and Management**	**P1**	**Low** **Moderate**

			High

Control Statement

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the HHS Standard for Encryption of Computing Device and organizationally-defined requirements (defined in, or referenced by, the applicable System Security and Privacy Plan) for key generation, distribution, storage, access, and destruction.

Discussion

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and specify appropriate options, parameters, and levels. Organizations manage trust stores to ensure that only approved trust anchors are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems. [NIST CMVP] and [NIST CAVP] provide additional information on validated cryptographic modules and algorithms that can be used in cryptographic key management and establishment.

Implementation Standard

High, Moderate & Low:

Std. 1 - When cryptographic mechanisms are needed, the information system must use encryption products that have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2 in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Control Review Frequency	**Assessment Frequency**
Quarterly	Annually (365 days)
Related Controls	**Reference Policy**
AC-17, AU-9, AU-10, CM-3, IA-3, IA-7, SA-4, SA-8, SA-9, SC-8, SC-11, SC-13, SC-17, SC-20, SC-37, SC-40, SI-3, SI-7	None;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SC-12(01)	**Availability**	**P1**	**High**

Control Statement

Maintain availability of information in the event of the loss of cryptographic keys by users.

Discussion

Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys. A forgotten passphrase is an example of losing a cryptographic key.

Implementation Standard

High:

Std.1 - Mechanisms are employed to:

(a) Prohibit the use of encryption keys that are not recoverable by authorized personnel;

(b) Require senior management approval to authorize recovery of keys by other than the key owner; and

(c) Comply with approved cryptography standards (see SC-13).

Control Review Frequency	**Assessment Frequency**
Monthly	Annually (365 days)
Related Controls	**Reference Policy**
None;	See Control SC-12;

Privacy Discussion

Privacy Implementation Standards

High:

<table>
<tr><td>Std.1 - Mechanisms are employed to:
(a) Prohibit the use of encryption keys that are not recoverable by authorized personnel;
(b) Require senior management approval to authorize recovery of keys by other than the key owner; and
(c) Comply with approved cryptography standards (see SC-13).</td></tr>
<tr><td><b>HVA Control Statement</b></td></tr>
<tr><td><b>HVA Discussion</b></td></tr>
<tr><td><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>SC-13</b></td><td><b>Control Name</b>
<b>Cryptographic Protection</b></td><td colspan="2"><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="5"><b>Control Statement</b>
a. Determine the defined cryptographic uses; and
b. Implement cryptographic mechanisms, in transit and at rest, for each specified cryptographic use as defined in the HHS Standard for Encryption of Computing Devices and Information, and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.</td></tr>
<tr><td colspan="5"><b>Discussion</b>
Cryptography can be employed to support a variety of security solutions, including the protection of classified information and controlled unclassified information, the provision and implementation of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals. Cryptography can also be used to support random number and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. For example, organizations that need to protect classified information may specify the use of NSA-approved cryptography. Organizations that need to provision and implement digital signatures may specify the use of FIPS-validated cryptography. Cryptography is implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
This control applies to applications with an integrated access control mechanism, such as WinZip and SecureZip, as well as the underlying operating system. These applications must meet CMS (FIPS 140-2 validated module) requirements.</td></tr>
<tr><td colspan="5"><b>Implementation Standard</b>
High, Moderate & Low:
Std. 1 - a. Determine the defined cryptographic uses; and
b. Implement cryptographic mechanisms, in transit and at rest, for each specified cryptographic use as defined in the HHS Standard for Encryption of Computing Devices and Information, and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Quarterly</td><td colspan="3"><b>Assessment Frequency</b>
Annually (365 days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-8, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SC-40, SI-3, SI-7</td><td colspan="3"><b>Reference Policy</b>
None;</td></tr>
<tr><td colspan="5"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="5"><b>Privacy Implementation Standards</b>
Guidance for systems processing, storing, or transmitting PII (to include PHI):
FIPS-validated cryptographic modules are the government standard for encryption. When sensitive information such as PII requires encryption, the organization must comply with these standards.
Guidance for systems processing, storing, or transmitting PHI:</td></tr>
</table>

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization. However, using cryptographic protection allows the organization to utilize the “Safe Harbor” provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **SC-15**	**Control Name** **Collaborative Computing Devices and Applications**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative; and

b. Provide an explicit indication of use to users physically present at the devices.

If collaborative computer is authorized, the authorization must specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used.

Discussion

Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.

Implementation Standard

High, Moderate & Low:

Std. 1 -   a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative; and

b. Provide an explicit indication of use to users physically present at the devices.

If collaborative computer is authorized, the authorization must specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used.

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 days)

Related Controls
AC-21, SC-42
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-3, AS-2;

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **SC-17**	**Control Name** **Public Key Infrastructure Certificates**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement a. Issue public key certificates under an appropriate certificate policy or obtain public key certificates from an approved service provider; and b. Include only approved trust anchors in trust stores or certificate stores managed by the organization	
Discussion Public key infrastructure (PKI) certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates. Reference: HHS Standard for Encryption of Computing Devices and Information	
Implementation Standard High & Moderate: Std. 1 - a. Issue public key certificates under an appropriate certificate policy or obtain public key certificates from an approved service provider; and b. Include only approved trust anchors in trust stores or certificate stores managed by the organization	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 days)

Related Controls
AU-10, IA-5, SC-12,
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-2, AS-2;
	NIST SP: 800-32, 800-63-3, 800-57-1, 800-57-2, 800-57-3,800-63-3;
	OMB Memo: M-05-24;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SC-18**	**Control Name** **Mobile Code**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**
Control Statement a. Define acceptable and unacceptable mobile code and mobile code technologies; and b. Authorize, monitor, and control the use of mobile code within the system.			
Discussion Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.			
Implementation Standard High & Moderate: Std. 1 - The CMS Technical Review Board (TRB) has the authority to permit or deny the use of mobile code. Std. 2 - The Organization (Enterprise) must comply with the federal guidelines in NIST SP 800-28 Guidelines on Active Content and Mobile Code, as amended.			
Control Review Frequency		**Assessment Frequency**	

Quarterly	Annually (365 days)

Related Controls
AU-2, AU-12, CM-2, CM-6, SI-3
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-4, AS-2;
	NIST SP: 800-28;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SC-18(04)**	**Control Name** **Prevent Automatic Execution**	**Priority**	**CMS Baseline** **HVA**
Control Statement Prevent the automatic execution of mobile code in software applications and enforce defined actions (defined in applicable system security and privacy plans) prior to executing the code.			
Discussion Actions enforced before executing mobile code include prompting users prior to opening email attachments or clicking on web links. Preventing the automatic execution of mobile code includes disabling auto-execute features on system components that employ portable storage devices, such as compact discs, digital versatile discs, and universal serial bus devices.			
Implementation Standard High & Moderate: Std. 1 - Prevent the automatic execution of mobile code in software applications and enforce defined actions (defined in applicable system security and privacy plans) prior to executing the code.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls None.		**Reference Policy** See Control SC-18.	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Prevent the automatic execution of mobile code, on all HVA systems and system components, in software applications and enforce defined actions (defined in applicable system security and privacy plans) prior to executing the code. An example of this is disabling auto run features on system components.			
HVA Discussion Actions enforced before executing mobile code include prompting users prior to opening email attachments or clicking on web links. Preventing automatic execution of mobile code includes disabling auto execute features on system components employing portable storage devices such as Compact Disk, Digital Versatile Disks, and Universal Serial Bus devices.			
HVA Implementation Standard			

Control Number **SC-20**	**Control Name** **Secure Name/Address Resolution Service (Authoritative Source)**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and			

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	
Discussion Providing authoritative source information enables external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include domain name system (DNS) servers. Additional artifacts include DNS Security Extensions (DNSSEC) digital signatures and cryptographic keys. Authoritative data includes DNS resource records. The means for indicating the security status of child zones include the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data. For additional guidance, see HHS Policy for Domain Name System (DNS) and Domain Name System Security Extensions (DNSSEC) Services.	
Implementation Standard High, Moderate & Low: Std. 1 - a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 days)

Related Controls
AU-10, SC-8, SC-12, SC-13, SC-21, SC-22
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-2, AS-2;
	NIST SP: 800-81;
	OMB Memo: M-08-23;
	FIPS 140-3, FIPS 186-4, SP 800-81-2.

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SC-21	**Secure Name/Address Resolution Service (Recursive or Caching Resolver)**	**P1**	**Low** **Moderate** **High**
Control Statement Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.			
Discussion Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data. The information system also disables recursive lookups on all publicly accessible domain name system (DNS) servers For additional guidance, see HHS Policy for Domain Name System (DNS) and Domain Name System Security Extensions (DNSSEC) Services.			
Implementation Standard High, Moderate & Low: Std. 1 - Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.			

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 days)

Related Controls
SC-20, SC-22
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-2, AS-2;
	NIST SP: 800-81-2;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SC-22**	**Control Name** **Architecture and Provisioning for Name/Address Resolution Service**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.
Discussion Systems that provide name and address resolution services include domain name system (DNS) servers. To eliminate single points of failure in systems and enhance redundancy, organizations employ at least two authoritative domain name system servers—one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks, including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles (e.g., by address ranges and explicit lists).
Implementation Standard High, Moderate & Low: Std. 1 - Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 days)

Related Controls
SC-2, SC-20, SC-21, SC-24
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-2, AS-2;
	NIST SP: 800-81-2;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SC-23**	**Control Name** **Session Authenticity**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement Protect the authenticity of communications sessions.

Discussion Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against "man-in-the-middle" attacks, session hijacking, and the insertion of false information into sessions.	
Implementation Standard Moderate & High: Std. 1 - Protect the authenticity of communications sessions.	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 days)

Related Controls
AU-10, SC-8, SC-10, SC-11.
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AC-2, AS-2;
	NIST SP: 800-52, 800-77, 800-95; 800-113

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SC-24**	**Control Name** **Fail In Known State**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Fail to a System Owner-defined known-state for System Owner-defined types of failures on the System Owner-defined components while preserving System Owner-defined system state information in failure.			
Discussion Failure in a known state addresses security concerns in accordance with the mission and business needs of organizations. Failure in a known state prevents the loss of confidentiality, integrity, or availability of information in the event of failures of organizational systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving system state information facilitates system restart and return to the operational mode with less disruption of mission and business processes.			
Implementation Standard High: Std. 1 - Fail to a known secure system state for all failures on system components while preserving the maximum amount of system state information in failure.			
Control Review Frequency Monthly		**Assessment Frequency** Annually (365 days)	
Related Controls CP-2, CP-4, CP-10, CP-12, SA-8, SC-7, SC-22, SI-13		**Reference Policy** None;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SC-28**	**Control Name** **Protection of Information At Rest**	**Priority** **P1**	**CMS Baseline** **Moderate** **High** **HVA**

Control Statement

Protect the confidentiality and integrity of information at rest, as defined in the HHS Standard for Encryption of Computing Devices and Information.

Discussion

Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing write-once-read-many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure offline storage in lieu of online storage.

Implementation Standard

High, Moderate & Low:

Std. 1 - Confidentiality and Integrity of information at rest must be protected in accordance with the HHS Standard for Encryption of Computing Devices and Information.

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 days)
Related Controls AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7----AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-12, SC-13, SC-34, SI-3, SI-7, SI-16	**Reference Policy** [OMB A-130], [SP 800-56A], [SP 800-56B], [SP 800-56C], [SP 800-57-1], [SP 800-572], [SP 800-57-3], [SP 800-111], [SP 800-124]

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

Protect the confidentiality and integrity of information/ HVA data-at-rest (DAR), as defined in the HHS Standard for Encryption of Computing Devices and Information, to prevent unauthorized access or exfiltration of HVA data. This control applies to workstations, servers, database stores, database repositories, information stores, portable media, and share drives.

HVA Discussion

Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information requiring protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authenticator content. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure off-line storage in lieu of online storage.

HVA Implementation Standard

Control Number **SC-28(01)**	**Control Name** **Cryptographic Protection**	**Priority** **P3**	**CMS Baseline** **Moderate** **High** **HVA**

Control Statement

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of CMS Sensitive Information at rest on system components or media.

Discussion

The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields.

For additional Guidance, see: HHS Standard for Encryption of Computing Devices and Information.

Implementation Standard

Moderate & High:

Std. 1 - When cryptographic mechanisms are required, the information system must utilize encryption products that have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2, as amended, in accordance with applicable federal laws, executive orders, directives, policies, regulations, and standards.

Control Review Frequency	**Assessment Frequency**
Annually (365 days)	Three (3) Years
Related Controls	**Reference Policy**

AC-19, SC-12, SC-13.	Code: 5 U.S.C. §552a(b) and (e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	OMB Memo: M-06-16, M-17-12 Att. 1, C.,
	HIPAA: 45 C.F.R. §164.312(a)(2)(iv), 45 C.F.R.§164.312(e)(2)(ii);

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

Implement cryptographic mechanisms to protect the confidentiality and integrity of HVA information at rest and prevent unauthorized disclosure and modification of information at rest on HVA.

HVA Discussion

Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information contained within the HVA. The strength of the cryptographic mechanism should be commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on HVA components or media or encrypt data structures, including files, records, or fields. The organization may leverage CDM Data Protection Management tools and methods to protect HVA information at rest.

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
SC-39	**Process Isolation**	**P1**	**Low** **Moderate** **High**

Control Statement

Maintain a separate execution domain for each executing process.

Discussion

Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. Process isolation helps limit the access of potentially

untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies.	
Implementation Standard High, Moderate & Low: Std. 1 - Maintain a separate execution domain for each executing process.	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 days)
Related Controls AC-3, AC-4, AC-6, AC-25, SA-8, SC-2, SC-3, SI-16.	**Reference Policy** FedRAMP: Rev. 4 Baseline; NIST SP 800-160-1
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

System and Information Integrity

Control Number	Control Name	Priority	CMS Baseline
SI-01	Policy and Procedures	P1	Low Moderate High

Control Statement

(a) Develop, document, and disseminate to applicable personnel and roles:

1. CMS Enterprise-level system and information integrity policy that:
    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the system and information integrity policy and associated SI controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

(c) Review and update the current system and information integrity:

1. Policy at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

System and information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and information integrity policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines

CMS provides an enterprise level System and Information Integrity policy within CMS IS2P2, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures).

Implementation Standard

High, Moderate & Low:

Std.1 - The CIO and CISO will provide leadership and oversight to: (a) Develop, document, and disseminate to applicable stakeholder personnel via the IS2P2:

1. CMS Enterprise-level system and information integrity policy that:
    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the system and information integrity policy and associated SI controls;

(b) Designate CMS-defined officials (e.g., CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

(c) Review and update the current system and information integrity:

1. Policy at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and

2. Procedures at least every three (3) years and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls
PM-9, PS-8, SA-8, S!-12
	Reference Policy
	Code: 5 U.S.C. §552a(b)and (e)(10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-1, SM-1, SM-3;
	HIPAA: 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.308(a)(5)(ii)(B), 45 C.F.R.§164.308(a)(6)(ii);
	NIST SP: 800-12, 800-100;
	OMB Memo: M-17-12; [OMB A-130]

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SI-02**	**Control Name** **Flaw Remediation**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates as directed in Implementation Standard 1; and d. Incorporate flaw remediation into the organizational configuration management process.			
Discussion The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified. Organization-defined time-periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw); the organizational mission; or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, for example, when implementing simple malicious code signature updates. Organizations consider in testing decisions whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.			
Implementation Standard High, Moderate & Low: Std.1 - Correct identified security-related information system flaws on production equipment based on frequency in applicable system's patch management plan. (a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes; and (b) Manage the flaw remediation process centrally.			

Std.2 - A risk-based decision is documented through the configuration management process in the form of written authorization from the CMS CIO or his/her designated representative (e.g., the system data owner or CMS CISO) and updated documentation in the risk analysis and security plan if a security patch is not to be applied to an information technology component or a legacy (no-longer maintained by the vendor) component is to remain in use.
Std.3 - Flaw remediation requirements apply to all information technology components for which a patch or work-around exists for each vendor-identified and/or CVE/CWE - identified vulnerability.
Std.4 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational flaw (e.g., patch) status and posture information.

Control Review Frequency	**Assessment Frequency**
Quarterly	Annually (365 Days)

Related Controls
CA-2, CA-5, CA-7, CM-3, CM-4, CM-5, CM-6, CM-8, IR-4, MA-2, RA-5, SA-8, SA-10, SA-11, SI-5, SI-7 SI-11
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-3, CM-5;
	HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(B);
	NIST SP: 800-40, 800-37, 800-39, 800-137, 800-128, 800-182;
	OMB Memo: M-14-03, M-16-04, M-19-03, M-20-04; OMB A-130,
	Binding Operational Directive 19-02 (BOD 19-02)
	FIPS: 140-3, 186-4.

Privacy Discussion

Privacy Implementation Standards

High, Moderate & Low:
Std.1 - Correct identified security-related information system flaws on production equipment within ten (10) business days and all others within thirty (30) calendar days.
(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes; and
(b) Manage the flaw remediation process centrally.
Std.2 - A risk-based decision is documented through the configuration management process in the form of written authorization from the CMS CIO or his/her designated representative (e.g., the system data owner or CMS CISO) and updated documentation in the risk analysis and security plan if a security patch is not to be applied to an information technology component or a legacy (no-longer maintained by the vendor) component is to remain in use.
Std.3 - Flaw remediation requirements apply to all information technology components for which a patch or work-around exists for each vendor-identified and/or CVE/CWE - identified vulnerability.
Std.4 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational flaw (e.g., patch) status and posture information.

HVA Control Statement

a. Identify, report, and correct HVA system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates as directed in Implementation Standard 1; and
d. Incorporate flaw remediation into the organizational change management processes and mitigates critical vulnerabilities on Internet facing systems in no more than 15 days.
e. Prioritize flaw remediation based on vulnerability exposure and criticality risk.
f. Define regular maintenance windows for flaw remediation.
g. Tests patches prior to production deployments, include identification and automated inventory of all software, hardware, and firmware and addresses flaws for all items inventoried.

HVA Discussion

The need to remediate system flaws applies to all types of software and firmware. Organizations should identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Organizations should also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified.

HVA Implementation Standard

Flaw remediation policies, procedures, and processes must be in accordance with CISA Binding Operational Directive (BOD) 19-02 on Vulnerability Remediation Requirements for Internet-Accessible Systems.

<table>
<tr><td><b>Control Number</b>
SI-02(02)</td><td><b>Control Name</b>
Automated Flaw Remediation Status</td><td><b>Priority</b>
P1</td><td><b>CMS Baseline</b>
Moderate
High</td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Determine if system components have applicable security-relevant software and firmware updates installed using automated mechanisms no less often than once every seventy-two hours.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Automated mechanisms can track and determine the status of known flaws for system components.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
Moderate & High:
Std.1 - Verify identified security-related information system flaws once every seventy-two (72) hours.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Quarterly</td><td colspan="2"><b>Assessment Frequency</b>
Annually (365 Days)</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
CM-7, SI-4</td><td colspan="2"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
NIST SP: 800-37, 800-39, 800-137;
OMB Memo: M-14-03, M-16-04, M-19-03, M-20-04;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
S1-02(06)</td><td><b>Control Name</b>
Removal of Previous Versions of Software and Firmware</td><td><b>Priority</b></td><td><b>CMS Baseline</b>
Above Baseline</td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Remove previous versions of software and firmware components after updated versions have been installed.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Previous versions of software or firmware components that are not removed from the system after updates have been installed may be exploited by adversaries. Some products may automatically remove previous versions of software and firmware from the system.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b></td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Not Specified</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
None.</td><td colspan="2"><b>Reference Policy</b>
See Control SI-2.</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="4"><b>HVA Discussion</b></td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
SI-03</td><td><b>Control Name</b>
Malicious Code Protection</td><td><b>Priority</b>
P1</td><td><b>CMS Baseline</b>
Low
Moderate
High</td></tr>
</table>

			HVA

Control Statement

a. Implement signature based and/or non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;
b. Automatically update malicious code protection mechanisms as new releases are available in accordance with CMS configuration management policy and procedures;
c. Configure malicious code protection mechanisms to:
1. Perform periodic scans of the system using the frequency specified in Implementation Standard 1 and Implementation Standard 2, and real-time scans of files from external sources at endpoint, and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational policy; and
2. Block and/or quarantine malicious code, take action in Implementation Standard 3 and send alert to administrator in response to malicious code detection; and
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Discussion

System entry and exit points include firewalls, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the world-wide web, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code.

Malicious code protection mechanisms include both signature- and nonsignature-based technologies. Nonsignature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Nonsignature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software and in custom-built software and could include logic bombs, back doors, and other types of attacks that could affect organizational missions and business functions.

In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended. Organizations may determine in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, or actions in response to detection of maliciousness when attempting to open or execute files.

Implementation Standard

High, Moderate & Low:
Std.1 - Desktop malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours.
Std.2 - Server (to include databases and applications) malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours.
Std.3 - Malicious code scanning results are reported to the CCIC SIEM in compliance with AU-06.

Control Review Frequency Monthly	**Assessment Frequency** Annually (365 Days)

Related Controls
AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, RA-5, SC-7, SC-23, SC-26, SC-28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15, PL-9
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	FISCAM: AS-3, CM-5;
	HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(B), 45 C.F.R. §164.308(a)(6)(ii);
	NIST SP: 800-37, 800-39, 800-83, 800-137;
	OMB Memo: M-14-03, M-16-04, M-19-03, M-20-04;
	[SP 800-83], [SP 800-125B], [SP 800-177].

Privacy Discussion

Privacy Implementation Standards

High, Moderate & Low:

Std.1 - Desktop malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours.
Std.2 - Server (to include databases and applications) malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours.
Std.3 - Malicious code scanning results are reported to the CCIC SIEM in compliance with AU-06.

HVA Control Statement

a. Implement signature based and/or non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;
b. Automatically update malicious code protection mechanisms as new releases are available in accordance with CMS configuration management policy and procedures;
c. Configure malicious code protection mechanisms to:
1. Perform periodic scans of the system at least biweekly, and real-time scans of files from external sources at endpoint, and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational policy; and
2. Block and quarantine malicious code and send alert to administrator in response to malicious code detection; and
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

HVA Discussion

System entry and exit points include firewalls, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, trojan horses, and spyware and can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography.

HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SI-04	**System Monitoring**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

a. Monitor the system to detect:
1. Attacks and indicators of potential attacks in accordance with the defined monitoring objectives listed in the CMS Incident Response Procedures and
2. Unauthorized local, network, and remote connections;
b. Identify unauthorized use of the system through defined techniques and methods (defined in the applicable System Security and Privacy Plan);
c. Invoke internal monitoring capabilities or deploy monitoring devices:
1. Strategically within the system to collect organization-determined essential information; and
2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Analyze detected events and anomalies;
e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
f. Obtain legal opinion regarding system monitoring activities; and
g. Provide defined system monitoring information (defined in the applicable System Security and Privacy Plan) to defined personnel or roles (defined in the applicable System Security and Privacy Plan) as needed, and at defined frequency (defined in the applicable System Security and Privacy Plan) as needed;

Discussion

System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at system boundaries. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capability is achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

Depending on the security architecture implementation, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries, and at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms supporting critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs and output from system monitoring serves as input to those programs. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other controls (e.g., AC-2g, AC-2(7), AC-2(12)(a), AC-17(1), AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, MA-3a, MA-4a, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18c, SC-43b). Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Implementation Standard

High, Moderate & Low:

Std.1 - Implement a centrally managed Intrusion detection system/intrusion protection system (IDS/IPS) capability to monitor network communications on all networks and subnets of any environment requiring a CMS Authority to Operate.

a. Permitted IDS/IPS mechanisms:

- centrally managed IDS/IPS devices at network perimeter points, to include between zones; and
- centrally managed host-based IDS/IPS sensor agents in information technology components for which such agents are available.

b. Environments where communications within the zone are encrypted must use mechanisms capable of either decrypting content for analysis or analyzing content before transmission/after receipt; and

c. Information technology components that do not support host-based IDS/IPS sensors capability must be documented in the applicable risk assessment and security plan.

Std.2 - Monitoring functionality supports the sharing of threat awareness information in a format that meets CMS requirements.

Std.3 - The organization monitors for unauthorized remote connections to the information system continuously, in real-time and takes appropriate action if an unauthorized connection is discovered.

Control Review Frequency Daily	**Assessment Frequency** Annually (365 Days)
Related Controls AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10	**Reference Policy** [OMB A-130], [FIPS 140-3], [SP 800-61], [SP-800-83], [SP-800-92], [SP 800-94], [SP 800-137]

Privacy Discussion

Privacy Implementation Standards

High, Moderate & Low:

Std.1 - Implement a centrally managed Intrusion detection system/intrusion protection system (IDS/IPS) capability to monitor network communications on all networks and subnets of any environment requiring a CMS Authority to Operate.

a. Permitted IDS/IPS mechanisms:

- centrally managed IDS/IPS devices at network perimeter points, to include between zones; and
- centrally managed host-based IDS/IPS sensor agents in information technology components for which such agents are available.

b. Environments where communications within the zone are encrypted must use mechanisms capable of either decrypting content for analysis or analyzing content before transmission/after receipt; and

c. Information technology components that do not support host-based IDS/IPS sensors capability must be documented in the applicable risk assessment and security plan.

Std.2 - Monitoring functionality supports the sharing of threat awareness information in a format that meets CMS requirements.

Std.3 - The organization monitors for unauthorized remote connections to the information system continuously, in real-time and takes appropriate action if an unauthorized connection is discovered.

HVA Control Statement

a. Monitor the system to detect:
1. Attacks and indicators of potential attacks in accordance with the defined monitoring objectives listed in the CMS Incident Response Procedures and
2. Unauthorized local, network, and remote connections;
b. Identify unauthorized use of the system through defined techniques and methods (defined in the applicable System Security and Privacy Plan);
c. Invoke internal monitoring capabilities or deploy monitoring devices:
1. Strategically within the system to collect organization-determined essential information; and
2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Analyze detected events and anomalies;
e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
f. Obtain legal opinion regarding system monitoring activities; and
g. Provides defined system monitoring information (defined in the applicable System Security and Privacy Plan) to defined personnel or roles (defined in the applicable System Security and Privacy Plan) as needed, and at defined frequency (defined in the applicable System Security and Privacy Plan) as needed;
h. Monitor the environment for both internal and external threats leveraging monitoring information from the boundary devices, isolation devices, workstation and server devices, and intrusion/prevention devices.
i. The HVA environment should be monitored for anomalous traffic, exfiltration, and indicators of insider threat.

HVA Discussion

System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at system boundaries while internal monitoring includes the observation of events occurring within the system. Organizations should monitor systems for example, by observing audit activities in cyber-relevant time or by observing other system aspects such as access patterns, characteristics of access, and other actions. System monitoring capability is achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
SI-04(01)	**System-Wide Intrusion Detection System**	**P3**	**HVA**

Control Statement

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

Discussion

Linking individual intrusion detection tools into a system-wide intrusion detection system provides additional coverage and effective detection capability. The information contained in one intrusion detection tool can be shared widely across the organization making the system-wide detection capability more robust and powerful.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Implementation Standard

High:
Std.1 - Aggregated intrusion detection information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; and
(b) Information sources include all network and host-based IDS/IPS capabilities monitoring network communications on all networks and subnets of any environment requiring a CMS Authority to Operate.
(c) CCIC directed aggregated intrusion detection information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw intrusion detection information must be available in an unaltered format to the CCIC.

Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years

Related Controls
None;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	NIST SP: 800-137;
	OMB Memo: M-14-03, M-20-04;

Privacy Discussion

Privacy Implementation Standards

High:
Std.1 - Aggregated intrusion detection information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; and
(b) Information sources include all network and host-based IDS/IPS capabilities monitoring network communications on all networks and subnets of any environment requiring a CMS Authority to Operate.
(c) CCIC directed aggregated intrusion detection information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw intrusion detection information must be available in an unaltered format to the CCIC.
Moderate & Low:
Std.1 - Aggregated intrusion detection information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; and
(b) Information sources include all network and host-based IDS/IPS capabilities monitoring network communications on all networks and subnets of any environment requiring a CMS Authority to Operate.
Std.2 - As required by CMS, raw intrusion detection information must be available in an unaltered format to the CCIC.

HVA Control Statement

Connect and configure HVA environment wide intrusion detection tools/prevention tools and solutions for all capable devices. Host based intrusion/prevention solutions report centrally to be used for monitoring of anomalous traffic, exfiltration, and indicators of insider threat.

HVA Discussion

Linking individual intrusion detection tools into a system-wide intrusion detection system provides additional coverage and effective detection capability. The information contained in one intrusion detection tool can be shared widely across the organization making the system-wide detection capability more robust and powerful.

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
SI-04(02)	**Automated Tools and Mechanisms for Real-Time Analysis**	**P1**	**Moderate** **High**

Control Statement

Employ automated tools and mechanisms to support near real-time analysis of events.

Discussion

Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or Security Information and Event Management technologies that provide real time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Implementation Standard

High & Moderate:

Std.1 - Aggregated real-time analysis of events information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include events/notifications emanating from local analysis tools and directly from any information technology component in an environment requiring a CMS Authority to Operate; and
(c) CCIC directed real-time analysis of events information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw event information must be available in an unaltered format to the CCIC.

Control Review Frequency Daily	**Assessment Frequency** Annually (365 Days)

Related Controls
PM-23, PM-25
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	NIST SP: 800-137;
	OMB Memo: M-14-03, M-20-04;

Privacy Discussion

Privacy Implementation Standards

High & Moderate:
Std.1 - Aggregated real-time analysis of events information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include events/notifications emanating from local analysis tools and directly from any information technology component in an environment requiring a CMS Authority to Operate; and
(c) CCIC directed real-time analysis of events information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw event information must be available in an unaltered format to the CCIC.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **SI-04(04)**	**Control Name** **Inbound and Outbound Communications Traffic**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
(b) Monitor inbound and outbound communications traffic at a defined frequency (defined in the applicable System Security and Privacy Plan) for unusual or unauthorized activities or conditions.

Discussion

Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code within organizational systems or propagating among system components; the unauthorized exporting of information; or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components.

Implementation Standard

High & Moderate:
Std.1 - Aggregated inbound and outbound communications traffic information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include traffic analysis information from local analysis tools and directly from any information technology component in an environment requiring a CMS Authority to Operate; and

(c) CCIC directed aggregated inbound and outbound communications traffic information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw event information must be available in an unaltered format to the CCIC.

Control Review Frequency Daily	**Assessment Frequency** Annually (365 Days)

Related Controls
None;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	NIST SP: 800-137;
	OMB Memo: M-14-03, M-20-04;

Privacy Discussion

Privacy Implementation Standards

High & Moderate:
Std.1 - Aggregated inbound and outbound communications traffic information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include traffic analysis information from local analysis tools and directly from any information technology component in an environment requiring a CMS Authority to Operate; and
(c) CCIC directed aggregated inbound and outbound communications traffic information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw event information must be available in an unaltered format to the CCIC.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
SI-04(05)	**System-Generated Alerts**	**P1**	**Moderate** **High**

Control Statement

Alert defined personnel or roles (defined in the applicable System Security and Privacy Plan) when the following system generated indications of compromise or potential compromise occur:
a. Presence of malicious code;
b. Unauthorized export of information;
c. Signaling to an external information system; or
d. Potential intrusions.

Discussion

Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms; intrusion detection or prevention mechanisms; or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. This control enhancement addresses the security alerts generated by the system. Alternatively, alerts generated by organizations in SI-4(12) focus on information sources external to the system such as suspicious activity reports and reports on potential insider threats.

Implementation Standard

High & Moderate:

Std.1 - Aggregated alert information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include all alert-generating information technology components in an environment requiring a CMS Authority to Operate; and
(c) CCIC directed aggregated alert information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw event information must be available in an unaltered format to the CCIC.
Low:
Std.1 – When selected, aggregated alert information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; and
(b) Information sources include all alert-generating information technology components in an environment requiring a CMS Authority to Operate.
Std.2 - When selected, as required by CMS, raw event information must be available in an unaltered format to the CCIC.

Control Review Frequency Daily	**Assessment Frequency** Annually (365 Days)

Related Controls
AU-4, AU-5, PE-6
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	NIST SP: 800-137;
	OMB Memo: M-14-03, M-20-04;

Privacy Discussion

Privacy Implementation Standards

High & Moderate:
Std.1 - Aggregated alert information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include all alert-generating information technology components in an environment requiring a CMS Authority to Operate; and
(c) CCIC directed aggregated alert information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw event information must be available in an unaltered format to the CCIC.
Low:
Std.1 – When selected, aggregated alert information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; and
(b) Information sources include all alert-generating information technology components in an environment requiring a CMS Authority to Operate.
Std.2 - When selected, as required by CMS, raw event information must be available in an unaltered format to the CCIC.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
SI-04(10)	**Visibility of Encrypted Communications**		**High** **HVA**

Control Statement

Make provisions so that encrypted communications traffic is visible to defined system monitoring tools and mechanisms.

Discussion

Organizations balance the need for encrypting communications traffic to protect data confidentiality with the need for having visibility into such traffic from a monitoring perspective. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.

<table>
<tr><td colspan="2">**Implementation Standard**
Moderate & High:
Std. 1 - Make provisions so that encrypted communications traffic is visible to defined system monitoring tools and mechanisms.</td></tr>
<tr><td>**Control Review Frequency**
Not Specified</td><td>**Assessment Frequency**
Three (3) Years</td></tr>
<tr><td>**Related Controls**
None.</td><td>**Reference Policy**
See Control SI-4.</td></tr>
<tr><td colspan="2">**Privacy Discussion**</td></tr>
<tr><td colspan="2">**Privacy Implementation Standards**</td></tr>
<tr><td colspan="2">**HVA Control Statement**
Make provisions so that encrypted communications traffic is visible and inspected to ensure that the traffic is legitimate and not exfiltration of data. Organizations should determine the best approach to mitigating the risks associated with encrypted traffic. Examples include choosing to limit encrypted traffic to only authorized encrypted connections and locations, encrypted traffic entering and leaving the environment with unknown or public sources, or destinations is decrypted and inspected to determine the appropriateness of use and unencrypt inbound traffic at known locations so it can be inspected and block all outbound unauthorized encrypted traffic.</td></tr>
<tr><td colspan="2">**HVA Discussion**
Organizations should balance the need for encrypting communications traffic to protect data confidentiality with the need for having visibility into such traffic from a monitoring perspective. Organizations can determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.</td></tr>
<tr><td colspan="2">**HVA Implementation Standard**</td></tr>
</table>

<table>
<tr><td>**Control Number**
SI-04(11)</td><td>**Control Name**
Analyze Communications Traffic Anomalies</td><td>**Priority**</td><td>**CMS Baseline**
HVA</td></tr>
<tr><td colspan="4">**Control Statement**
Analyze outbound communications traffic at the external interfaces to the system and selected interior points within the system (defined in the applicable System Security and Privacy Plan) to discover anomalies.</td></tr>
<tr><td colspan="4">**Discussion**
Organization-defined interior points include subnetworks and subsystems. Anomalies within organizational systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols (e.g. IPv6 usage during IPv4 transition), and attempted communications with suspected malicious external addresses.</td></tr>
<tr><td colspan="4">**Implementation Standard**
Moderate & High:
Std. 1 - Analyze outbound communications traffic at the external interfaces to the system and selected interior points within the system (defined in the applicable System Security and Privacy Plan) to discover anomalies.</td></tr>
<tr><td colspan="2">**Control Review Frequency**
Not Specified</td><td colspan="2">**Assessment Frequency**
Three (3) Years</td></tr>
<tr><td colspan="2">**Related Controls**
None.</td><td colspan="2">**Reference Policy**
See Control SI-4.</td></tr>
<tr><td colspan="4">**Privacy Discussion**</td></tr>
<tr><td colspan="4">**Privacy Implementation Standards**</td></tr>
<tr><td colspan="4">**HVA Control Statement**
Analyze outbound communications traffic at the external interfaces to the system and selected interior points within the system (defined in the applicable System Security and Privacy Plan) to discover anomalies.
The organization should monitor outbound and inbound traffic at the authorization boundary as well as strategic points inside the environment, such as boundary protection devices isolating the tiers (enclaves) to detect for anomalies, malicious traffic, or threats.</td></tr>
<tr><td colspan="4">**HVA Discussion**</td></tr>
</table>

Organization-defined interior points include subnetworks and subsystems. Anomalies within organizational systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols (e.g., IPv6 usage during IPv4 transition), and attempted communications with suspected malicious external addresses.
HVA Implementation Standard

Control Number **SI-04(12)**	**Control Name** **Automated Organization-Generated Alerts**	**Priority**	**CMS Baseline** **High**
Control Statement Alert applicable personnel or roles using automated mechanisms (defined in the applicable System Security and Privacy Plan) when indications of inappropriate or unusual activities with security or privacy implications occur.			
Discussion Organizational personnel on the system alert notification list include system administrators, mission or business owners, system owners, senior agency information security officer, senior agency official for privacy, system security officers, or privacy officers. This control enhancement focuses on the security alerts generated by organizations and transmitted using automated means. In contrast to the alerts generated by systems in SI-4(5) that focus on information sources that are internal to the systems such as audit records, the sources of information for this enhancement focus on other entities such as suspicious activity reports and reports on potential insider threats.			
Implementation Standard High: Std. 1 - Alert applicable personnel or roles using automated mechanisms (defined in the applicable System Security and Privacy Plan) when indications of inappropriate or unusual activities with security or privacy implications occur.			
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years		
Related Controls SI-4(5)	**Reference Policy** See Control SI-4.		
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SI-04(13)**	**Control Name** **Analyze Traffic and Event Patterns**	**Priority**	**CMS Baseline** **HVA**
Control Statement (a) Analyze communications traffic and event patterns for the system; (b) Develop profiles representing common traffic and event patterns; and (c) Use the traffic and event profiles in tuning system-monitoring devices.			
Discussion Identifying and understanding common communications traffic and event patterns helps organizations provide useful information to system monitoring devices to more effectively identify suspicious or anomalous traffic and events when they occur. Such information can help reduce the number of false positives and false negatives during system monitoring.			
Implementation Standard Moderate & High: Std. 1 - (a) Analyze communications traffic and event patterns for the system; (b) Develop profiles representing common traffic and event patterns; and (c) Use the traffic and event profiles in tuning system-monitoring devices.			

Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls None.	**Reference Policy** OMB Circular A-130 NIST SP 800-61 Rev 2, NIST SP 800-92, NIST SP 800-137
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement (a) Analyze communications traffic and event patterns for the system at the authorization boundary and at access control points inside the environment, such as boundary protection devices isolated the tiers (enclaves). (b) Develop profiles representing common traffic patterns and actions; and (c) Use the traffic and event profiles in monitoring traffic in these same locations and use the baselines as a comparison to detect for unusual traffic. (d) Configure detection monitoring tools with these baseline characteristics to alert on threshold values.	
HVA Discussion Identifying and understanding common communications traffic and event patterns helps organizations provide useful information to system monitoring devices to more effectively identify suspicious or anomalous traffic and events when they occur. Such information can help reduce the number of false positives and false negatives during system monitoring.	
HVA Implementation Standard	

Control Number **SI-04(14)**	**Control Name** **Wireless Intrusion Detection**	**Priority** **P3**	**CMS Baseline** **High**
Control Statement Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.			
Discussion Wireless signals may radiate beyond organizational facilities. Organizations proactively search for unauthorized wireless connections, including the conduct of thorough scans for unauthorized wireless access points. Wireless scans are not limited to those areas within facilities containing systems, but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational systems.			
Implementation Standard High: Std. 1 - Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls AC-18, IA-3		**Reference Policy** FedRAMP: Rev. 4 Baseline; GAO: Finding TBS	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SI-04(16)**	**Control Name** **Correlate Monitoring Information**	**Priority** **P3**	**CMS Baseline** **HVA**
Control Statement Correlate information from monitoring tools and mechanisms employed throughout the system.			

Discussion Correlating information from different system monitoring tools and mechanisms can provide a more comprehensive view of system activity. Correlating system monitoring tools and mechanisms that typically work in isolation, including malicious code protection software, host monitoring, and network monitoring, can provide an organization-wide monitoring view and may reveal otherwise unseen attack patterns. Understanding capabilities and limitations of diverse monitoring tools and mechanisms and how to maximize the utility of information generated by those tools and mechanisms can help organizations to develop, operate, and maintain effective monitoring programs. Correlation of monitoring information is especially important during the transition from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).	
Implementation Standard Moderate & High: Std. 1 - Correlate information from monitoring tools and mechanisms employed throughout the system.	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years

Related Controls
AU-6
	Reference Policy
	Statute: Cybersecurity Enhancement Act of 2014;
	FedRAMP: Rev. 4 Baseline;
	OMB Memo: M-14-03, M-20-04;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement The organization should correlate information from monitoring tools and mechanisms employed throughout the enterprise.	
HVA Discussion Organizations should correlate monitoring information from enterprise monitoring tools and mechanisms such as, but not limited to antivirus monitoring, Intrusion Detection System, Intrusion Prevention System, logging, etc. Organizations should protect this information at the level commensurate with the highest level of information contained within.	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SI-04(18)	**Analyze Traffic and Covert Exfiltration**		**HVA**

Control Statement Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: defined interior points within the system.	
Discussion Organization-defined interior points include subnetworks and subsystems. Covert means that can be used to exfiltrate information include steganography.	
Implementation Standard Moderate & High: Std. 1 - Correlate information from monitoring tools and mechanisms employed throughout the system.	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls None.	**Reference Policy** OMB Circular A-130 NIST SP 800-61 Rev 2, NIST SP 800-92, NIST SP 800-137
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement The organization should monitor, inspect and analyze outbound communications traffic at the HVA authorization boundary and at strategic locations inside the boundary to detect covert exfiltration of information.	
HVA Discussion	

<table>
<tr><td>Organization-defined HVA system interior points should include both subnetwork and subsystem information. Covert means that can be used to exfiltrate information include steganography.</td></tr>
<tr><td><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>SI-04(20)</b></td><td><b>Control Name</b>
<b>Privileged Users</b></td><td colspan="2"><b>Priority</b></td><td><b>CMS Baseline</b>
<b>High</b>
<b>HVA</b></td></tr>
<tr><td colspan="5"><b>Control Statement</b>
Implement the following additional monitoring of privileged users: e.g. audit record monitoring software, and network monitoring software.</td></tr>
<tr><td colspan="5"><b>Discussion</b>
Privileged users have access to more sensitive information, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to systems and organizations than non-privileged users. Therefore, implementing additional monitoring on privileged users helps to ensure that organizations can identify malicious activity at the earliest possible time and take appropriate actions.</td></tr>
<tr><td colspan="5"><b>Implementation Standard</b>
Moderate & High:
Std. 1 - Implement the following additional monitoring of privileged users: e.g. audit record monitoring software, and network monitoring software.</td></tr>
<tr><td colspan="3"><b>Control Review Frequency</b>
Not Specified</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="3"><b>Related Controls</b>
AC-18</td><td colspan="2"><b>Reference Policy</b>
See Control SI-4.</td></tr>
<tr><td colspan="5"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="5"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="5"><b>HVA Control Statement</b>
Implement additional monitoring of privileged users based on based on established policies. They should determine what additional monitoring attributes for privileged account are implemented based on risk assessment and potential impact to the environment. i.e., successful process execution, successful resource access, etc.</td></tr>
<tr><td colspan="5"><b>HVA Discussion</b>
Privileged users may have access to more HVA data, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to HVA systems and organizations than non-privileged users. Therefore, implementing additional monitoring on privileged users helps to ensure organizations can identify malicious activity at the earliest possible time and take appropriate actions.</td></tr>
<tr><td colspan="5"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>SI-04(22)</b></td><td><b>Control Name</b>
<b>Unauthorized Network Services</b></td><td colspan="2"><b>Priority</b></td><td><b>CMS Baseline</b>
<b>High</b>
<b>HVA</b></td></tr>
<tr><td colspan="5"><b>Control Statement</b>
(a) Detect network services that have not been authorized or approved by CMS CIO or Authorizing Official as identified in the applicable System Security and Privacy Plan; and
(b) Audit and/or alert applicable personnel or roles (e.g. ISSO, CCIC as defined within the System Security and Privacy Plan) when detected.</td></tr>
<tr><td colspan="5"><b>Discussion</b>
Unauthorized or unapproved network services include services in service-oriented architectures that lack organizational verification or validation and therefore may be unreliable or serve as malicious rogues for valid services.</td></tr>
<tr><td colspan="5"><b>Implementation Standard</b>
Moderate & High:
Std. 1 - (a) Detect network services that have not been authorized or approved by CMS CIO or Authorizing Official as identified in the applicable System Security and Privacy Plan; and
(b) Audit and/or alert applicable personnel or roles (e.g. ISSO, CCIC as defined within the System Security and Privacy Plan) when detected.</td></tr>
<tr><td colspan="3"><b>Control Review Frequency</b></td><td colspan="2"><b>Assessment Frequency</b></td></tr>
</table>

<table>
<tr><td>Not Specified</td><td>Three (3) Years</td></tr>
<tr><td><b>Related Controls</b>
CM-7</td><td><b>Reference Policy</b>
See Control SI-4.</td></tr>
<tr><td colspan="2"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="2"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="2"><b>HVA Control Statement</b>
(a) Define authorized network services, implement solutions to detect network services that have not been authorized or approved by authorization or approval processes (defined in the applicable System Security and Privacy Plan); and
(b) Create alerts and alert applicable personnel's when detected.</td></tr>
<tr><td colspan="2"><b>HVA Discussion</b>
Unauthorized or unapproved network services include services in service-oriented architectures that lack organizational verification or validation and therefore may be unreliable or serve as malicious rogues for valid services. Examples include peer-to-peer communications and Internet relay chat.</td></tr>
<tr><td colspan="2"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>SI-04(23)</b></td><td><b>Control Name</b>
<b>Host-Based Devices</b></td><td><b>Priority</b>
<b>P3</b></td><td><b>CMS Baseline</b>
<b>HVA</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Implement the following CMS-required host-based monitoring mechanisms on all systems, appliances, devices, services, and applications;
- Devices and appliances that do not support a host-based intrusion detection system/intrusion prevention system (IDS/IPS) sensor capability must be documented in the applicable Information System Risk Assessment and System Security and Privacy Plan.</td></tr>
<tr><td colspan="4"><b>Discussion</b>
System components where host-based monitoring can be implemented include servers, notebook computers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple product developers or vendors.</td></tr>
<tr><td colspan="4"><b>Implementation Standard</b>
Moderate & High:
Std. 1 - Implement the following additional monitoring of privileged users: e.g. audit record monitoring software, and network monitoring software.</td></tr>
<tr><td colspan="2"><b>Control Review Frequency</b>
Not Specified</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="2"><b>Related Controls</b>
AC-18, AC-19</td><td colspan="2"><b>Reference Policy</b>
FedRAMP: Rev. 4 Baseline;
NIST SP: 800-37, 800-39, 800-137;
OMB Memo: M-14-03, M-16-04, M-19-03, M-20-04;</td></tr>
<tr><td colspan="4"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="4"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="4"><b>HVA Control Statement</b>
Implement the following CMS-required host-based monitoring mechanisms within the HVA accreditation boundary;
- Devices and appliances that do not support a host-based intrusion detection system/intrusion prevention system (IDS/IPS) sensor capability must be documented in the applicable Information System Risk Assessment and System Security and Privacy Plan.</td></tr>
<tr><td colspan="4"><b>HVA Discussion</b>
System components where host-based monitoring can be implemented include servers, notebook computers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple product developers or vendors.</td></tr>
<tr><td colspan="4"><b>HVA Implementation Standard</b></td></tr>
</table>

Control Number	Control Name	Priority	CMS Baseline
SI-05	**Security Alerts, Advisories, and Directives**	**P1**	**Low** **Moderate** **High** **HVA**

Control Statement

a. Receive system security alerts, advisories, and directives from defined external organizations (including CISA, United States Computer Emergency Readiness Team (US-CERT) and organizations as defined in the applicable System Security and Privacy Plan)) on an ongoing basis;
b. Generate internal security alerts, advisories, and directives as deemed necessary;
c. Disseminate security alerts, advisories, and directives to: defined personnel or roles (defined in the applicable System Security and Privacy Plan); and
d. Implement security directives in accordance with established time frames, or notify CMS of the degree of noncompliance.

Discussion

The Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness throughout the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations.

Implementation Standard

High, Moderate & Low:
Std.1 - The organization's security operations center is responsible for responding to advisories, requests, or directives issued by the CMS Security Operations Center (SOC) and/or CCIC.
Std. 2 - The organization must adhere to HHS Policy for Vulnerability Management.

Control Review Frequency	Assessment Frequency
Quarterly	Annually (365 Days)

Related Controls	Reference Policy
SI-2, PM-15, RA-5	NIST SP 800-40.

Privacy Discussion

Privacy Implementation Standards

High, Moderate & Low:
Std.1 - The organization's security operations center is responsible for responding to advisories, requests, or directives issued by the CMS Security Operations Center (SOC) and/or CCIC.

HVA Control Statement

a. Receive system security alerts, advisories, and directives from defined external organizations (including CISA and organizations as defined in the applicable System Security and Privacy Plan) on an ongoing basis;
b. Generate internal security alerts, advisories, and directives as deemed necessary;
c. Disseminate HVA security alerts, advisories, and directives to the organization's HVA PMO staff and other key stakeholders; and
d. Implement security directives in accordance with established time frames, or notify CMS of the degree of noncompliance.

HVA Discussion

CISA generates security alerts and advisories to maintain situational awareness throughout the Federal Government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation if not implemented in a timely manner.

HVA Implementation Standard

Control Number **SI-05(01)**	**Control Name** **Automated Alerts and Advisories**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement Broadcast security alert and advisory information throughout the organization using automated mechanisms (defined in applicable system security/privacy plan).			
Discussion The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational missions and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three levels related to the management of information security and privacy risk, including the governance level, mission and business process level, and the information system level.			
Implementation Standard High: Std. 1 - Broadcast security alert and advisory information throughout the organization using automated mechanisms (defined in applicable system security/privacy plan).			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	
Related Controls None;		**Reference Policy** See Control SI-5;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SI-06**	**Control Name** **Security and Privacy Function Verification**	**Priority** **P1**	**CMS Baseline** **High**
Control Statement a. Verify the correct operation of defined security and privacy functions (defined in the applicable System Security Plan); b. Perform the verification of the functions specified in SI-6a upon system startup, restart, and upon command by a user with appropriate privileges no less often than once per month; c. Alert the system administrators to failed security and privacy verification tests; and d. Shut the information system down, restarts the system, or performs some other defined alternative action(s) (defined in the applicable System Security and Privacy Plan) when anomalies are discovered.			
Discussion Transitional states for systems include system startup, restart, shutdown, and abort. System notifications include hardware indicator lights, electronic alerts to system administrators, and messages to local computer consoles. In contrast to security function verification, privacy function verification ensures that privacy functions operate as expected and are approved by the senior agency official for privacy, or that privacy attributes are applied or used as expected.			
Implementation Standard High; Std. 1 - a. Verify the correct operation of defined security and privacy functions (defined in the applicable System Security Plan); b. Perform the verification of the functions specified in SI-6a upon system startup, restart, and upon command by a user with appropriate privileges no less often than once per month; c. Alert the system administrators to failed security and privacy verification tests; and d. Shut the information system down, restarts the system, or performs some other defined alternative action(s) (defined in the applicable System Security and Privacy Plan) when anomalies are discovered.			

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)
Related Controls CA-7, CM-4, CM-6, SI-7	**Reference Policy** [OMB A-130]
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SI-07**	**Control Name** **Software, Firmware, and Information Integrity**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement a. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: e.g., parity checks, cyclical redundancy checks, cryptographic hashes.			
Discussion Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes the Basic Input Output System (BIOS). Information includes personally identifiable information and metadata containing security and privacy attributes associated with information. Integrity-checking mechanisms, including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools can automatically monitor the integrity of systems and hosted applications.			
Implementation Standard High & Moderate: Std. 1 - a. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: e.g., parity checks, cyclical redundancy checks, cryptographic hashes.			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	
Related Controls AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11		**Reference Policy** [OMB A-130], [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], NIST: [SP 800-70], [SP 800-147]	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SI-07(01)**	**Control Name** **Integrity Checks**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Perform an integrity check of software, firmware, and information: at startup and/or at transitional states or at security-relevant events; at least quarterly.			

Discussion Security-relevant events include the identification of a new threat to which organizational systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort.	
Implementation Standard High & Moderate: Std. 1 - Perform an integrity check of software, firmware, and information: at startup and/or at transitional states or at security-relevant events; at least quarterly.	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)
Related Controls None;	**Reference Policy** FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
SI-07(02)	**Automated Notifications of Integrity Violations**	**P1**	**High**

Control Statement Employ automated tools that provide notification to defined personnel or roles (defined in the applicable System Security Plan) upon discovering discrepancies during integrity verification.	
Discussion The employment of automated tools to report system and information integrity violations and to notify organizational personnel in a timely matter is essential to effective risk response. Personnel having an interest in system and information integrity violations include mission and business owners, system owners, senior agency information security official, senior agency official for privacy, systems administrators, software developers, systems integrators, and information security officers, and privacy officers.	
Implementation Standard High: Std. 1 - Employ automated tools that provide notification to defined personnel or roles (defined in the applicable System Security Plan) upon discovering discrepancies during integrity verification.	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)
Related Controls None;	**Reference Policy** See Control SI-7;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	Control Name	Priority	CMS Baseline
SI-07(05)	**Automated Response to Integrity Violations**	**P1**	**High**
Control Statement			

Automatically implements one or more of the security safeguards defined in Implementation Standard 1 when integrity violations are discovered. Implemented controls must be specified in the applicable System Security Plan.

Discussion

Organizations may define different integrity checking responses by type of information, by specific information, or a combination of both. Types of information include firmware, software, and user data. Specific information includes boot firmware for certain types of machines. The automatic implementation of controls within organizational systems includes reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur.

Implementation Standard

High:
Std.1 - One or more of the following safeguards must be implemented when integrity violations are discovered:
(a) Shut the information system down;
(b) Restart the information system; or
(c) Implement security and/or privacy controls defined in the System Security and Privacy Plan.

Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)
Related Controls None;	**Reference Policy** See Control SI-7;

Privacy Discussion

Privacy Implementation Standards

High:
Std.1 - One or more of the following safeguards must be implemented:
(a) Shuts the information system down;
(b) Restarts the information system; or
(c) Implements the security safeguards defined in the System Security and Privacy Plan.

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number **SI-07(07)**	**Control Name** **Integration of Detection and Response**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: e.g. unauthorized changes to established CMS configuration settings or the unauthorized elevation of system privileges.

Discussion

Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

Implementation Standard

High & Moderate:
Std. 1 - Incorporate the detection of the following unauthorized changes into the organizational incident response capability: e.g. unauthorized changes to established CMS configuration settings or the unauthorized elevation of system privileges.

Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years

Related Controls AU-2, AU-6, IR-4, IR-5, SI-4	**Reference Policy** See Control SI-7.
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SI-07(15)**	**Control Name** **Code Authentication**	**Priority**	**CMS Baseline** **High**
Control Statement Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: Implement Standards in Implementation Standards 1 and 2.			
Discussion Cryptographic authentication includes verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code. Organizations employing cryptographic mechanisms also consider cryptographic key management solutions (see SC-12 and SC-13). FIPS-validated cryptographic modules are the government standard for encryption. The Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/Projects/cryptographic-module-validation-program) validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules.			
Implementation Standard High: Std. 1 - Encryption products must be validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2 in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Std. 2 - Cryptographic mechanisms must be implemented in accordance with the HHS Standard for Encryption of Computing Devices and Information.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls CM-5, SC-12, SC-13		**Reference Policy** See Control SI-7;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SI-08**	**Control Name** **Spam Protection**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**
Control Statement a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.			
Discussion System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions. At CMS, suspicious email must be reported to spam@cms.hhs.gov or using the 'Report Phishing' icon on the CMS Microsoft Outlook mail client interface.			
Implementation Standard			

High & Moderate: Std. 1 - a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)
Related Controls PL-9,SC-5, SC-7, SC-38, SI-3, SI-4	**Reference Policy** [SP 800-45], [SP 800-177, HHS Policy for Internet and Email Security
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SI-08(02)**	**Control Name** **Automatic Updates**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**

Control Statement Automatically update spam protection mechanisms on a regular basis (as defined the System Security and Privacy Plan).	
Discussion Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capability.	
Implementation Standard High & Moderate: Std. 1 - Automatically update spam protection mechanisms on a regular basis (as defined the System Security and Privacy Plan).	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)
Related Controls None;	**Reference Policy** See Control SI-8.
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SI-10**	**Control Name** **Information Input Validation**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**

Control Statement Check the validity of defined information inputs (defined in the applicable System Security Plan) for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.
Discussion Checking the valid syntax and semantics of system inputs, including character set, length, numerical range, and acceptable values, verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of 387, abc, or %K% are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications

typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.	
Implementation Standard High & Moderate: Std. 1 - Check the validity of defined information inputs (defined in the applicable System Security Plan) for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls
None;
	Reference Policy
	FedRAMP: Rev. 4 Baseline;
	OMB A-130
	FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SI-11**	**Control Name** **Error Handling**	**Priority** **P2**	**CMS Baseline** **Moderate** **High**

Control Statement a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and b. Reveal error messages only to defined personnel or roles (defined in the applicable System Security and Privacy Plan).	
Discussion Organizations consider the structure and the content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.	
Implementation Standard High & Moderate: Std. 1 - a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and b. Reveal error messages only to defined personnel or roles (defined in the applicable System Security and Privacy Plan).	
Control Review Frequency Quarterly	**Assessment Frequency** Annually (365 Days)

Related Controls
AU-2, AU-3, SC-31, SI-2, SI-15
	Reference Policy
	Code: 5 U.S.C. §552a(e)(5) and (10);
	Statute: Privacy Act of 1974 (P.L. 93-579);
	FedRAMP: Rev. 4 Baseline;
	FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2;
	OMB Circular: A-130 7.g.;
	HIPAA: 45 C.F.R. §164.308(a)(3)(i);

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
SI-12	**Information Management and Retention**	**P2**	**Low** **Moderate** **High**

Control Statement

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

Discussion

Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, and other types of administrative information. The National Archives and Records Administration (NARA) provides federal policy and guidance on records retention. If organizations have a records management office, consider coordinating with records management personnel.

Implementation Standard

High, Moderate & Low:

Std.1 - Retain output, including but not limited to audit records, system reports, business and financial reports, and business records from the information system in accordance with CMS Policy and all applicable NARA requirements.

Control Review Frequency	Assessment Frequency
Annually (365 Days)	Three (3) Years
Related Controls	**Reference Policy**
AC-16, AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PL-2, PL-4, PM-4, PM-8, PM-9, PS-2, PS-6, PT-2, PT3, RA-2, RA-3, SA-5, SA-8, SR-2.	[USC 2901], [OMB A-130, Appendix II]

Privacy Discussion

Privacy Implementation Standards

High, Moderate & Low:

Std.1 - Retain output, including but not limited to audit records, system reports, business and financial reports, and business records from the information system in accordance with CMS Policy and all applicable NARA requirements.

Systems processing, storing, or transmitting PHI:

PHI.1 - HIPAA requires that the following actions, activities, and assessments relating to the security of systems containing PHI be documented and retained for at least six years from the date of its creation or the date when it was last in effect, whichever is later:

- Decisions regarding addressable implementation specifications, specifically why it would not be reasonable and appropriate to implement the implementation specification in question;
- A user’s right of access to a workstation, transaction, program, or process;
- Security incidents and their outcomes;
- Satisfactory assurances that a business associate will appropriately safeguard PHI. This documentation is recorded in a written contract or other arrangement with the business associate and must meet the applicable requirements of business associate agreements. If satisfactory assurances cannot be attained, document the attempt and the reasons that these assurances cannot be obtained;
- Repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks); and
- Changes to organizational policies and procedures.

HVA Control Statement

HVA Discussion
HVA Implementation Standard

Control Number **SI-12(01)**	**Control Name** **Limit Personally Identifiable Information Elements**	**Priority**	**CMS Baseline** **Moderate** **High**
Control Statement Limit personally identifiable information being processed in the information life cycle to defined elements of Personally Identifiable Information, e.g. name, social security number, date and place of birth, mother's maiden name, or biometric records.			
Discussion Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for operational purposes helps to reduce the level of privacy risk created by a system. The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining which elements of personally identifiable information may create risk.			
Implementation Standard High & Moderate: Std.1 - Limit personally identifiable information being processed in the information life cycle to defined elements of Personally Identifiable Information, e.g. name, social security number, date and place of birth, mother's maiden name, or biometric records.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls PM-25, PT-2, PT-3, RA-3		**Reference Policy** See Control SC-12.	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SI-12(02)**	**Control Name** **Minimize Personally Identifiable Information in Testing, Training, and Research**	**Priority**	**CMS Baseline** **Moderate** **High**
Control Statement Use the techniques in accordance with the CMS Privacy Handbook and applicable federal laws and regulations to minimize the use of personally identifiable information for research, testing, or training.			
Discussion Organizations can minimize the risk to an individual's privacy by employing techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining the techniques to use and when to use them.			
Implementation Standard High & Moderate: Std.1 - Use the techniques in accordance with the CMS Privacy Handbook and applicable federal laws and regulations to minimize the use of personally identifiable information for research, testing, or training.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls		**Reference Policy**	

PM-22, PM-25, SI-19	See Control SC-12.
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SI-12(03)**	**Control Name** **Information Disposal**	**Priority**	**CMS Baseline** **Moderate** **High**
Control Statement Use NIST SP 800-88 techniques to dispose of, destroy, or erase information following the retention period.			
Discussion Organizations can minimize both security and privacy risks by disposing of information when it is no longer needed. Disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.			
Implementation Standard High & Moderate: Std.1 - Use NIST SP 800-88 techniques to dispose of, destroy, or erase information following the retention period.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls MP-6		**Reference Policy** See Control SI-12.	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SI-16**	**Control Name** **Memory Protection**	**Priority** **P1**	**CMS Baseline** **Moderate** **High**
Control Statement Implement the following controls to protect the system memory from unauthorized code execution: controls defined in applicable system security and privacy plan (e.g. data execution prevention controls). Implemented safeguards must be specified in the applicable system security and privacy plan.			
Discussion Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.			
Implementation Standard High & Moderate: Std. 1 - Implement the following controls to protect the system memory from unauthorized code execution: controls defined in applicable system security and privacy plan (e.g. data execution prevention controls). Implemented safeguards must be specified in the applicable system security and privacy plan.			
Control Review Frequency Quarterly		**Assessment Frequency** Annually (365 Days)	
Related Controls		**Reference Policy**	

AC-25, SC-3, SI-7	FedRAMP: Rev. 4 Baseline;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SI-18**	**Control Name** **Personally Identifiable Information Quality Operations**	**Priority**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle no less often than once every 365 days or as directed by the HHS Data Integrity Board; and b. Correct or delete inaccurate or outdated personally identifiable information.			
Discussion Personally identifiable information quality operations include the steps that organizations take to confirm the accuracy and relevance of personally identifiable information throughout the information life cycle. The information life cycle includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information. Personally identifiable information quality operations include editing and validating addresses as they are collected or entered into systems using automated address verification look-up application programming interfaces. Checking personally identifiable information quality includes the tracking of updates or changes to data over time, which enables organizations to know how and what personally identifiable information was changed should erroneous information be identified. The measures taken to protect personally identifiable information quality are based on the nature and context of the personally identifiable information, how it is to be used, how it was obtained, and potential de-identification methods employed. The measures taken to validate the accuracy of personally identifiable information used to make determinations about the rights, benefits, or privileges of individuals covered under federal programs may be more comprehensive than the measures used to validate personally identifiable information used for less sensitive purposes. Note- The PIA should be checked and updated for any changes to the PII in the system.			
Implementation Standard High, Moderate & Low: Std. 1 - a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle no less often than once every 365 days or as directed by the HHS Data Integrity Board; and b. Correct or delete inaccurate or outdated personally identifiable information.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls PM-22, PM-24, SI-4, PT-2		**Reference Policy** SP 800-188, IR 8112, OMB M-19-15	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SI-18(04)**	**Control Name** **Individual Requests**	**Priority**	**CMS Baseline** **Moderate** **High**
Control Statement Correct or delete personally identifiable information upon request by individuals or their designated representatives.			
Discussion			

Inaccurate personally identifiable information maintained by organizations may cause problems for individuals, especially in those business functions where inaccurate information may result in inappropriate decisions or the denial of benefits and services to individuals. Even correct information, in certain circumstances, can cause problems for individuals that outweigh the benefits of an organization maintaining the information. Organizations use discretion in determining if personally identifiable information is to be corrected or deleted, based on the scope of requests, the changes sought, the impact of the changes, and applicable laws, regulations, and policies. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding appropriate instances of correction or deletion.

Implementation Standard

High & Moderate:

Std. 1 - Correct or delete personally identifiable information upon request by individuals or their designated representatives.

Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls PM-22	**Reference Policy** See Control SI-18.

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion

HVA Implementation Standard

Control Number	Control Name	Priority	CMS Baseline
SI-19	**De-Identification**		**Moderate** **High**

Control Statement

a. Remove the following examples of elements of personally identifiable information from datasets: name, social security number, date and place of birth, mother's maiden name, or biometric records; and

b. Evaluate using frequency (defined in applicable System Security and Privacy Plan) for effectiveness of de-identification.

Discussion

De-identification is the general term for the process of removing the association between a set of identifying data and the data subject. Many datasets contain information about individuals that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. Datasets may also contain other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Personally identifiable information is removed from datasets by trained individuals when such information is not (or no longer) necessary to satisfy the requirements envisioned for the data. For example, if the dataset is only used to produce aggregate statistics, the identifiers that are not needed for producing those statistics are removed. Removing identifiers improves privacy protection, since information that is removed cannot be inadvertently disclosed or improperly used. Organizations may be subject to specific de-identification definitions or methods under applicable laws, regulations, or policies. Re-identification is a residual risk with de-identified data. Re-identification attacks can vary including combining new datasets or other improvements in data analytics. Maintaining awareness of potential attacks and evaluating for the effectiveness of the de-identification over time supports management of this residual risk.

Implementation Standard

High & Moderate:

Std. 1 - a. Remove the following examples of elements of personally identifiable information from datasets: name, social security number, date and place of birth, mother's maiden name, or biometric records; and

b. Evaluate using frequency (defined in applicable System Security and Privacy Plan) for effectiveness of de-identification.

Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls MP-6, PM-22, PM-23, PM-24, RA-2, SI-12	**Reference Policy** OMB A-130 Appendix II NIST SP 800-188

Privacy Discussion

Privacy Implementation Standards

HVA Control Statement

HVA Discussion
HVA Implementation Standard

Supply Chain Risk Management

Control Number	Control Name	Priority	CMS Baseline
SR-01	**Policy and Procedures**	**P1**	**Low** **Moderate** **High**

Control Statement

(a) Develop, document, and disseminate to applicable personnel and roles:
1. CMS Enterprise-level supply chain risk management policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;
(b) Designate CMS-defined officials (e.g., SCRM Manager, CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and
(c) Review and update the current supply chain risk management:
1. Policy annually and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and
2. Procedures annually and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

Discussion

Supply chain risk management policy and procedures address the controls in the SR family as well as supply chain-related controls in other families that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of supply chain risk management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to supply chain risk management policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Policies, processes, and procedures associated with SR control family will enable CMS to leverage a holistic approach that both identifies stakeholders within the enterprise and identifies the risks to CMS and CMS data throughout the supply chain.

CMS provides an enterprise supply chain risk management policy within this IS2P2, and procedures within the RMH, that can be inherited by CMS organizations and systems. Risk-based customization is recommended when the CMS organizational or system level security and privacy needs (i.e., special requirements exist that are unique to the CMS organization or system) are not fully addressed by the enterprise policy. (Implemented policy must not be less stringent than the enterprise policy and procedures.)

Implementation Standard

High, Moderate & Low:

Std.1 - The CIO and CISO will provide leadership and oversight to: (a) Develop, document, and disseminate to applicable stakeholder personnel via the IS2P2:
1. CMS Enterprise-level supply chain risk management policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;
(b) Designate CMS-defined officials (e.g., SCRM Manager, CMS Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and
(c) Review and update the current supply chain risk management:
1. Policy annually and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines); and

2. Procedures annually and following CMS-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).	
Control Review Frequency Annually (365 Days)	**Assessment Frequency** Three (3) Years
Related Controls PM-9, PM-30, PS-8, SI-12;	**Reference Policy** NIST SP: 800-12, 800-30, 800-39, 800-100, 800-161; FASC18, 41 CFR 201, EO 13873
Privacy Discussion Discussion for systems processing, storing, or transmitting PII (to include PHI): Privacy considerations should be included in supply chain risk management policy and procedures, especially when the system contains information subject to the Privacy Act and/or HIPAA.	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SR-02**	**Control Name** **Supply Chain Risk Management Plan**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement (a) Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the CMS systems, system components or system services. (b) Review and update the supply chain risk management plan annually or as required, to address threat, organizational or environmental changes; and (c) Protect the supply chain risk management plan from unauthorized disclosure and modification.			
Discussion The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders. Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints and implications. It can either be stand-alone, or incorporated into system security and privacy plans. The SCRM plan addresses managing, implementation, and monitoring of SCRM controls and the development/sustainment of systems across the SDLC to support mission and business functions. Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose, and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment. Supply chain risk management plans include an expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, a description of and justification for supply chain risk mitigation measures taken, and associated roles and responsibilities. Finally, supply chain risk management plans address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes (see SA-8).			
Implementation Standard High, Moderate & Low: Std. 1 - The Supply chain risk management (SCRM) plan must address managing, implementation, and monitoring of SCRM controls, identified in NIST SP 800-53 rev5, and the development/sustainment of systems across the CMS TLC to support mission and business functions.			
Control Review Frequency		**Assessment Frequency**	

Not Specified	Three (3) Years
Related Controls CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4.	**Reference Policy** NIST SP: 800-30, 800-39, 800-160 v1, 800-161, 800-181; NISTIR: 7622; 8272 FASC18, 41 CFR 201, EO 13873, CNSSD 505.
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SR-02(01)	**Establish SCRM Team**	**P1**	**Low** **Moderate** **High**

Control Statement

Establish a supply chain risk management team consisting of CMS personnel, with roles and responsibilities defined in the CMS IS2P2, to lead and support the following SCRM activities: OIT (defined through CIO-level policies) and CMS defined supply chain risk management activities (defined in applicable security/privacy plans).

Discussion

To implement supply chain risk management plans, organizations establish a coordinated, team-based approach to identify and assess supply chain risks and manage these risks by using programmatic and technical mitigation techniques. The team approach enables organizations to conduct an analysis of their supply chain, communicate with internal and external partners or stakeholders, and gain broad consensus regarding the appropriate resources for SCRM. The SCRM team consists of organizational personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executive, information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions. Members of the SCRM team are involved in various aspects of the SDLC and, collectively, have an awareness of and provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems. The SCRM team can be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

At CMS, the SCRM Awareness Group (SCRMAG) is headed by the Division of Strategic Information (DSI) with the support of the Office of Acquisition and Grants Management (OAGM). These offices are responsible for ensuring a secure supply chain through inclusion of appropriate contract clauses. The CMS SCRMAG is as an intra-agency communication and outreach organization designed to facilitate the exchange of supply chain risk-related information across the enterprise. This information will include potential supply chain threats and risks to CMS assets, as well as, countermeasures and mitigations.

Implementation Standard

High, Moderate & Low:

Std. 1 - Establish a supply chain risk management team consisting of CMS personnel, with roles and responsibilities defined in the CMS IS2P2, to lead and support the following SCRM activities: OIT (defined through CIO-level policies) and CMS defined supply chain risk management activities (defined in applicable security/privacy plans).

Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls None;	**Reference Policy** See Control SR-2;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

<table>
<tr><td><b>Control Number</b>
<b>SR-03</b></td><td colspan="2"><b>Control Name</b>
<b>Supply Chain Controls and Processes</b></td><td><b>Priority</b>
<b>P1</b></td><td><b>CMS Baseline</b>
<b>Low</b>
<b>Moderate</b>
<b>High</b></td></tr>
<tr><td colspan="5"><b>Control Statement</b>
(a) Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of Business/System-defined system or system component (defined in applicable security/privacy plans) in coordination with the CMS OIT, or designee, and the CMS CISO, or designee;
(b) Employ the following supply chain controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events:
1. OIT and CISO-defined supply chain controls (defined through CIO-level policies); and
2. Business/System-defined supply chain controls (defined in applicable security/privacy plans); and
(c) Document the selected and implemented supply chain processes and controls in applicable security/privacy plans as well as supply chain risk management plan.</td></tr>
<tr><td colspan="5"><b>Discussion</b>
Supply chain elements include organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components. Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components. Supply chain elements and processes may be provided by organizations, system integrators, or external providers. Weaknesses or deficiencies in supply chain elements or processes represent potential vulnerabilities that can be exploited by adversaries to cause harm to the organization and affect its ability to carry out its core missions or business functions. Supply chain personnel are individuals with roles and responsibilities in the supply chain.</td></tr>
<tr><td colspan="5"><b>Implementation Standard</b>
High, Moderate & Low:
Std. 1 - The organization must comply with guidelines detailed in the HHS Policy for Cyber Supply Chain Risk Management.</td></tr>
<tr><td colspan="3"><b>Control Review Frequency</b>
Not Specified</td><td colspan="2"><b>Assessment Frequency</b>
Three (3) Years</td></tr>
<tr><td colspan="3"><b>Related Controls</b>
CA-2, MA-2, MA-6, PE-3, PE-16, PL-8, PM-30, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SC-7, SC-29, SC-30, SC-38, SI-7, SR-6, SR-9, SR-11;</td><td colspan="2"><b>Reference Policy</b>
NIST SP: 800-30, 800-161;
NISTIR: 7622;
FASC18, 41 CFR 201, EO 13873, ISO 20243</td></tr>
<tr><td colspan="5"><b>Privacy Discussion</b></td></tr>
<tr><td colspan="5"><b>Privacy Implementation Standards</b></td></tr>
<tr><td colspan="5"><b>HVA Control Statement</b></td></tr>
<tr><td colspan="5"><b>HVA Discussion</b></td></tr>
<tr><td colspan="5"><b>HVA Implementation Standard</b></td></tr>
</table>

<table>
<tr><td><b>Control Number</b>
<b>SR-04(02)</b></td><td><b>Control Name</b>
<b>Track and Trace</b></td><td><b>Priority</b>
<b>P2</b></td><td><b>CMS Baseline</b>
<b>HVA</b></td></tr>
<tr><td colspan="4"><b>Control Statement</b>
Establish and maintain unique identification of the following systems and critical system components for tracking through the supply chain:
(a) OIT- and CISO-defined systems and critical system components (defined through CIO-level policies); and
(b) Business/System-defined systems and critical system components (defined in applicable security/privacy plans).</td></tr>
<tr><td colspan="4"><b>Discussion</b>
Tracking the unique identification of systems and system components during development and transport activities provides a foundational identity structure for the establishment and maintenance of provenance. For example, system components may be labeled using serial numbers or tagged using radio-frequency identification tags. Labels and tags can help provide better visibility into the provenance of a system or system component. A system or system component may have more than one unique identifier. Identification methods are sufficient to support a forensic investigation after a supply chain compromise or event.</td></tr>
</table>

Implementation Standard High & Moderate: Std. 1 - Establish and maintain unique identification of the following systems and critical system components for tracking through the supply chain: (a) OIT- and CISO-defined systems and critical system components (defined through CIO-level policies); and (b) Business/System-defined systems and critical system components (defined in applicable security/privacy plans).	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls IA-2, IA-8, PE-16, PL-2;	**Reference Policy** See SR-4;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement 1. Establish and maintain unique identification of the following HVA systems and critical system components for tracking through the supply chain: (a) OIT- and CISO-defined systems and critical system components (defined through CIO-level policies); and (b) Business/System-defined systems and critical system components (defined in applicable MAC security/privacy plans). 2. Reduce HVA supply chain risks by tracking each HVA and HVA component (as applicable) from the origin by creating and assigning unique identifiers.	
HVA Discussion Labels (e.g. serial numbers) and tags (e.g. radio-frequency identification tags) can help provide better visibility into the provenance of the HVA or HVA component. The HVA or HVA component may have more than one unique identifier and these identification methods should be sufficient to support a forensic investigation after a supply chain compromise or event.	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SR-04(03)	**Validate as Genuine and Not Altered**	**P2**	**HVA**

Control Statement Employ controls in accordance with the HHS Policy for Cyber Supply Chain Risk Management (Appendix A) to validate that the system or system component received is genuine and has not been altered.	
Discussion For many systems and system components, especially hardware, there are technical means to determine if the items are genuine or have been altered, including optical and nanotechnology tagging, physically unclonable functions, side-channel analysis, cryptographic hash verifications or digital signatures, and visible anti-tamper labels or stickers. Controls can also include monitoring for out of specification performance, which can be an indicator of tampering or counterfeits. Organizations may leverage supplier and contractor processes for validating that a system or component is genuine and has not been altered and for replacing a suspect system or component. Some indications of tampering may be visible and addressable before accepting delivery, such as inconsistent packaging, broken seals, and incorrect labels. When a system or system component is suspected of being altered or counterfeit, the supplier, contractor, or original equipment manufacturer may be able to replace the item or provide a forensic capability to determine the origin of the counterfeit or altered item. Organizations can provide training to personnel on how to identify suspicious system or component deliveries.	
Implementation Standard High & Moderate: Std. 1 - Employ controls in accordance with the HHS Policy for Cyber Supply Chain Risk Management (Appendix A) to validate that the system or system component received is genuine and has not been altered.	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls AT-3, SR-9, SR-10, SR-11;	**Reference Policy** See SR-4;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	

Employ controls in accordance with the HHS Policy for Cyber Supply Chain Risk Management (Appendix A) to validate that the HVA system or system component received is genuine and conduct testing to validate the HVA or HVA component received is genuine and has not been altered along the organization's supply chain.
HVA Discussion Controls can also include monitoring for out of specification performance, which can be an indicator of tampering or counterfeits. Organizations may leverage supplier and contractor processes for validating that a system or component is genuine and has not been altered, and for replacing a suspect system or component. Some indications of tampering may be visible and addressable before accepting delivery. When the HVA or HVA component is suspected of being altered or counterfeit, the supplier, contractor, or original equipment manufacturer may be able to replace the item or provide a forensic capability to determine the origin of the counterfeit or altered item.
HVA Implementation Standard

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SR-05	**Acquisition Strategies, Tools, and Methods**	**P1**	**Low** **Moderate** **High**

Control Statement Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: (a) OIT- and CISO-defined acquisition strategies, contract tools, and procurement methods (defined through CIO-level policies); and (b) Business/System-defined acquisition strategies, contract tools, and procurement methods (defined in applicable security/privacy plans).
Discussion The use of the acquisition process provides an important vehicle to protect the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development life cycle. Organizations also consider providing incentives for suppliers who implement controls, promote transparency into their processes and security and privacy practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.
Implementation Standard High, Moderate & Low: Std. 1 - Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: (a) OIT- and CISO-defined acquisition strategies, contract tools, and procurement methods (defined through CIO-level policies); and (b) Business/System-defined acquisition strategies, contract tools, and procurement methods (defined in applicable security/privacy plans).

Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years

Related Controls
AT-3, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SR-6, SR-9, SR-10, SR-11;
	Reference Policy
	NIST SP: 800-30, 800-161;
	NISTIR: 7622, 8272;
	FASC18, 41 CFR 201, EO 13873, ISO 27036, ISO 20243

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **SR-05(02)**	**Control Name** **Assessments Prior to Selection, Acceptance, Modification, or Update**	**Priority** **P2**	**CMS Baseline** **HVA**
Control Statement Assess the system, system component, or system service prior to selection, acceptance, modification, or update.			
Discussion Organizational personnel or independent, external entities conduct assessments of systems, components, products, tools, and services to uncover evidence of tampering, unintentional and intentional vulnerabilities, or evidence of non-compliance with supply chain controls. These include malicious code, malicious processes, defective software, backdoors, and counterfeits. Assessments can include evaluations; design proposal reviews; visual or physical inspection; static and dynamic analyses; visual, x-ray, or magnetic particle inspections; simulations; white, gray, or black box testing; fuzz testing; stress testing; and penetration testing (see SR-6(1)). Evidence generated during assessments is documented for follow-on actions by organizations. The evidence generated during the organizational or independent assessments of supply chain elements may be used to improve supply chain processes and inform the supply chain risk management process. The evidence can be leveraged in follow-on assessments. Evidence and other documentation may be shared in accordance with organizational agreements.			
Implementation Standard High & Moderate: Std. 1 - Assess the system, system component, or system service prior to selection, acceptance, modification, or update.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls CA-8, RA-5, SA-11, SI-7, SR-9;		**Reference Policy** See SR-5;	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Assess the HVA system, system component, or system service prior to selection, acceptance, modification, and/or update			
HVA Discussion Evidence of tampering or vulnerabilities could include malicious code or processes, defective software, backdoors, and counterfeits. Assessments can include evaluations, design proposal reviews, visual or physical inspection, static and dynamic analyses, visual, x-ray, or magnetic particle inspections, simulations, white, gray, or black box testing, fuzz testing, stress testing, or penetration testing. Evidence generated during assessments should be documented for follow-on actions by organizations. The evidence generated during the organizational or independent assessments of supply chain elements may be used to improve supply chain processes and to inform the supply chain risk management process.			
HVA Implementation Standard			

Control Number **SR-06**	**Control Name** **Supplier Assessments and Reviews**	**Priority** **P1**	**CMS Baseline** **Moderate** **High** **HVA**
Control Statement Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide every 365 days.			
Discussion An assessment and review of supplier risk includes security and supply chain risk management processes, foreign ownership, control or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors. The reviews may be conducted by the organization or by an independent third party. The reviews consider documented processes, documented controls, all-source intelligence, and publicly available information related to the supplier or contractor. Organizations can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits. In some cases, it may be appropriate or required to share assessment and review results with other organizations in accordance with any applicable rules, policies, or inter-organizational agreements or contracts.			

At CMS, the reviews must ensure the vendors, or their products, have not been flagged as questionable (or restricted) by one or more Federal authorities (e.g., Kaspersky-branded products are disallowed by DHS BOD 17-01). The review must also include ensuring suppliers do not have questionable ties to foreign governments (this is FOCI).	
Implementation Standard High & Moderate: Std. 1 - Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide every 365 days.	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years

Related Controls
SR-3, SR-5;
	Reference Policy
	FIPS: 140-3, 180-4, 186-4, 202;
	NIST SP: 800-30, 800-161;
	NISTIR: 7622, 8272;
	FASC18, 41 CFR 201, EO 13873, ISO 27036, ISO 20243;

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide: a. before a one-time purchase of the HVA, component, or service; b. at least biannually for regularly purchased or long-term purchases of an, component, or service; and c. if possible, after a major breach or incident occurs with a supplier or contractor within the organization's supply chain.	
HVA Discussion A review of supplier risk includes security processes, foreign ownership, control or influence, and the ability of the supplier to effectively assess any subordinate second-tier and third-tier suppliers and contractors. The reviews may be conducted by the organization or by an independent third party. The reviews consider documented processes, documented controls, all-source intelligence, and publicly available information related to the supplier or contractor. Organizations can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits. In some cases, it may be appropriate to share review results with other organizations in accordance with any applicable agreements or contracts.	
HVA Implementation Standard	

Control Number **SR-08**	**Control Name** **Notification Agreements**	**Priority** **P1**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises, results of assessments or audits, and CMS information (defined in applicable security/privacy plans).			
Discussion The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.			
Implementation Standard High, Moderate & Low: Std. 1 - Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises, results of assessments or audits, and CMS information (defined in applicable security/privacy plans).			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls		**Reference Policy**	

IR-4, IR-6, IR-8;	NIST SP: 800-30, 800-161;
	NISTIR: 7622;
	FASC18, 41 CFR 201, EO 13873, ISO 27036

Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SR-09	**Tamper Resistance and Detection**	**P1**	**High** **HVA**
Control Statement Implement a tamper protection program for the system, system component, or system service.			
Discussion Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.			
Implementation Standard High: Std. 1 - Implement a tamper protection program for the system, system component, or system service.			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls PE-3, PM-30, SA-15, SI-4, SI-7, SR-3, SR-4, SR-5, SR-10, SR-11;		**Reference Policy** ISO 20243	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Implement a tamper protection program for the HVA system, system component, or system service to help with the detection of instances of tampering.			
HVA Discussion Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.			
HVA Implementation Standard			

Control Number	**Control Name**	**Priority**	**CMS Baseline**
SR-09(01)	**Multiple Stages of System Development Life Cycle**	**P2**	**High**
Control Statement Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.			
Discussion The system development life cycle includes research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal. Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations use obfuscation and self-checking to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. The customization of systems and system components can make substitutions easier to detect and therefore limit damage.			

Target Life Cycle (TLC) is CMS's system development life cycle governance process that promotes business flexibility, and replaces point-in-time gate reviews with continuous evaluation and situational reviews governance.	
Implementation Standard High: Std. 1 - Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls SA-3;	**Reference Policy** None;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Control Number **SR-10**	**Control Name** **Inspection of Systems or Components**	**Priority** **P2**	**CMS Baseline** **Low** **Moderate** **High** **HVA**
Control Statement Inspect the following systems or system components at random and/or every 365 days or upon indications of need for inspection to detect tampering: CMS systems and system components (defined in applicable security/privacy plans).			
Discussion The inspection of systems or systems components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from organization-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.			
Implementation Standard High, Moderate & Low: Std. 1 - Inspect the following systems or system components at random and/or every 365 days or upon indications of need for inspection to detect tampering: CMS systems and system components (defined in applicable security/privacy plans).			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls AT-3, PM-30, SI-4, SI-7, SR-3, SR-4, SR-5, SR-9, SR-11;		**Reference Policy** ISO 20243	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement Inspect the following HVA systems or system components at random and/or every 365 days, upon indications of need for inspection to detect tampering: CMS systems and system components (defined in applicable security/privacy plans).			
HVA Discussion Inspection of the HVA or HVA components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components taken out of organization-controlled areas. Indications of a need for inspection include when individuals return from travel to high-risk locations.			
HVA Implementation Standard			

Control Number **SR-11**	**Control Name** **Component Authenticity**	**Priority** **P2**	**CMS Baseline** **Low**

			Moderate **High**
Control Statement (a) Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and (b) Report counterfeit system components to the source of counterfeit component, the CMS CCIC, CISA, and CMS personnel or roles, e.g. CMS SCRM Manager (defined in applicable security/privacy plans and CMS IS2P2).			
Discussion Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policy and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. Internal reporting organizations include the CMS CCIC. External reporting organizations include CISA.			
Implementation Standard High, Moderate & Low: Std. 1 - (a) Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and (b) Report counterfeit system components to the source of counterfeit component, the CMS CCIC, CISA, and CMS personnel or roles, e.g. CMS SCRM Manager (defined in applicable security/privacy plans and CMS IS2P2).			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls PE-3, SA-4, SI-7, SR-9, SR-10;		**Reference Policy** NISTIR: 7622; ISO 20243.	
Privacy Discussion			
Privacy Implementation Standards			
HVA Control Statement			
HVA Discussion			
HVA Implementation Standard			

Control Number **SR-11(01)**	**Control Name** **Anti-counterfeit Training**	**Priority** **P2**	**CMS Baseline** **Low** **Moderate** **High**
Control Statement Train all System Engineers, ISSOs, System Owners and other System POCs as well CMS personnel or roles (defined in CMS IS2P2 and/or in applicable security/privacy plans) to detect counterfeit system components (including hardware, software, and firmware).			
Discussion Training employed by CMS Businesses/Systems to detect the counterfeit component use within the supply chain depends on the tool and industry standard that defines the inspection, test, and authentication (IT&A) used (see SR-11(3)). The five best known sources for SCRM standards used for IT&A include the Independent Distributors of Electronics Association (IDEA), the Joint Electron Device Engineering Council (JEDEC), Institute of Printed Circuits (IPC), the Society of Automotive Engineers (SAE) International, and the Defense Logistics Agency (DLA). Since each source defines its own criteria (e.g., sampling, non-destructive and destructive tests) for completion of the assessment, associated training will be unique to the selected criteria.			
Implementation Standard High, Moderate & Low: Std. 1 - Train all System Engineers, ISSOs, System Owners and other System POCs as well CMS personnel or roles (defined in CMS IS2P2 and/or in applicable security/privacy plans) to detect counterfeit system components (including hardware, software, and firmware).			
Control Review Frequency Not Specified		**Assessment Frequency** Three (3) Years	
Related Controls AT-3;		**Reference Policy** NISTIR: 7622; ISO 20243.	
Privacy Discussion			
Privacy Implementation Standards			

HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **SR-11(02)**	**Control Name** **Configuration Control for Component Service and Repair**	**Priority** **P2**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement

Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service:

(a) OIT- and CISO-defined system components (defined through CIO-level policies); and

(b) Business/System-defined system components (defined in applicable security/privacy plans).

Discussion

CMS Businesses/Systems achieve configuration control by developing, documenting, and maintaining a current baseline configuration of components (both components awaiting service or repair and components awaiting return to service).

This could be as rigorous as adopting a two-person rule for component and configuration changes where the changes cannot be reversed, or where non-repudiation of the change is not possible. Identify, document, and review any exceptions from the mandatory configuration settings for individual components based on the development, operational, and delivery requirements.

Implementation Standard

High, Moderate & Low:

Std. 1 - Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service:

(a) OIT- and CISO-defined system components (defined through CIO-level policies); and

(b) Business/System-defined system components (defined in applicable security/privacy plans).

Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls CM-3, MA-2, MA-4, SA-10;	**Reference Policy** NISTIR: 7622; ISO 20243.

Privacy Discussion
Privacy Implementation Standards
HVA Control Statement
HVA Discussion
HVA Implementation Standard

Control Number **SR-12**	**Control Name** **Component Disposal**	**Priority** **P2**	**CMS Baseline** **Low** **Moderate** **High**

Control Statement

Dispose of CMS data, documentation, tools or system components using the techniques and methods in accordance with NIST SP 800-88.

Discussion

Data, documentation, tools, or system components can be disposed of at any time during the system development life cycle (not only in the disposal or retirement phase of the life cycle). For example, disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, partial reuse of components. Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media, which contain sensitive or proprietary information. Additionally, proper disposal of system components helps to prevent such components from entering the gray market.

CMS Business/System components that have been used to process, transmit, or store CMS sensitive information and will not be leaving CMS control may be reused for the same purposes. If the system components will be repurposed (i.e., reused under different purposes) must be thoroughly sanitized (purged) according to CMS's media sanitization

policies. System components that will be leaving CMS control, especially systems components from systems that have processed, transmitted, or stored CMS sensitive information such as PII, must be either physically destroyed or thoroughly sanitized before disposal. Total destruction and proper sanitization of the components prior to disposal or release protects residual information from unauthorized use and disclosure. NIST SP 800-88, as amended, and the National Industrial Security Program's Operating Manual (DoD 5220.22-M, HYPERLINK "https://www.hsdl.org/?view&did=461297".) provide additional information on disposal approaches.	
Implementation Standard High, Moderate & Low: Std. 1 - Dispose of CMS data, documentation, tools or system components using the techniques and methods in accordance with NIST SP 800-88.	
Control Review Frequency Not Specified	**Assessment Frequency** Three (3) Years
Related Controls MP-6;	**Reference Policy** NISTIR: 7622;
Privacy Discussion	
Privacy Implementation Standards	
HVA Control Statement	
HVA Discussion	
HVA Implementation Standard	

Acceptable Risk Safeguards 5.0

Effective Date/Approval

This Standard becomes effective on the date that CMS's Chief Information Officer (CIO) sig and remains in effect until it is rescinded, or superseded.

Signature: Rajiv K. Uppal -S Digitally signed by Rajiv K. Uppal -S
Date: 2022.01.06 16:32:44 -05'00' Date of Issuance _

Rajiv Uppal
Chief Information Officer and
Director, Office of Information Technology(OIT)

Standard Owner's Review Certification

This document must be reviewed in accordance with CMS Policy

Signature: Robert M. Wood -S Digitally signed by Robert M. Wood -S
Date: 2022.01.06 10:06:40 -05'00' Date of Annual Review:

Robert Wood
CMS Chief Information Security Officer
Director, Information Security and Privacy Group

ns it

01/03/2022

ARS 5.0

Control Family	Control Number	Control Name	CMS ARS 5.0 Control
Access Control	AC-02(06)	Dynamic Privilege	Implement [CMS-defined dynamic privilege management capabilities].
Access Control	AC-02(08)	Dynamic Account	Create, activate, manage, and deactivate [Assignment: organization-defined system
Access Control	AC-03(02)	Dual Authorization	Enforce dual authorization for [CMS-defined privileged commands and/or other organization-defined actions].
Access Control	AC-03(03)	Mandatory Access Control	Enforce dual authorization for [Assignment: organization-defined privileged commands
Access Control	AC-03(04)	Discretionary Access Control	Enforce [CMS-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy, and where the policy specifies that a subject that has been granted access to information can do one or more of the following: (a) Pass the information to any other subjects or objects; (b) Grant its privileges to other subjects; (c) Change security attributes on subjects, objects, the system, or the system's components; (d) Choose the security attributes to be associated with newly created or revised objects; or (e) Change the rules governing access control.
Access Control	AC-03(05)	Security-Relevant Information	Prevent access to [CMS-defined security-relevant information] except during secure, non-operable system states.
Access Control	AC-03(07)	Role-Based Access Control	Enforce a role-based access control policy over defined subjects and objects and control access
Access Control	AC-03(08)	Revocation of Access Authorizations	Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [CMS-defined rules governing the timing of revocations of access authorizations].
Access Control	AC-03(10)	Audited Override of Access	Employ an audited override of automated access control mechanisms under [Assignment:
Access Control	AC-03(12)	Assert and Enforce Application Access	(a) Require applications to assert, as part of the installation process, the access needed to the system applications and functions (defined in applicable security and privacy plan): (b) Provide an enforcement mechanism to prevent unauthorized access; and
Access Control	AC-03(13)	Attribute-Based Access Control	Enforce attribute-based access control policy over defined subjects and objects and control access based upon defined attributes to assume access permissions (defined in applicable security and privacy plan).
Access Control	AC-03(15)	Discretionary and Mandatory Access Control	(a) Enforce CMS-defined mandatory access control policy over the set of covered subjects and objects specified in the policy; and (b) Enforce CMS-defined discretionary access control policy over the set of covered subjects and objects specified in the policy.
Access Control	AC-04(01)	Object Security and Privacy Attributes	Use [CMS-defined security and privacy attributes] associated with [CMS-defined information, source, and destination objects] to enforce [CMS-defined information flow control policies] as a basis for flow
Access Control	AC-04(02)	Processing Domains	Use protected processing domains to enforce [CMS-defined information flow control policies] as a basis for flow control decisions.
Access Control	AC-04(03)	Dynamic Information Flow Control	Enforce [CMS-defined information flow control policies].
Access Control	AC-04(05)	Embedded Data Types	Enforce [CMS-defined limitations] on embedding data types within other data types.
Access Control	AC-04(06)	Metadata	Enforce information flow control based on [CMS-defined metadata].
Access Control	AC-04(07)	One-way Flow Mechanisms	Enforce one-way information flows through hardware-based flow control mechanisms.
Access Control	AC-04(08)	Security and Privacy Policy Filters	(a) Enforce information flow control using defined security or privacy policy filters (defined in applicable security/privacy plans) as a basis for flow control decisions for prevention of unauthorized transfer of PII across information system boundaries or domains; and (b) Block, strip, modify, or quarantine data after a filter processing failure in accordance with applicable CMS security or privacy policy.
Access Control	AC-04(09)	Human Reviews	Enforce the use of human reviews for [CMS-defined information flows] under the following conditions: [CMS-defined conditions].
Access Control	AC-04(10)	Enable and Disable Security or Privacy Policy Filters	Provide the capability for privileged administrators to enable and disable [CMS-defined security or privacy policy filters] under the following conditions: [Assignment: organization-defined conditions].
Access Control	AC-04(11)	Configuration of Security or Privacy Policy Filters	Provide the capability for privileged administrators to configure [CMS-defined security or privacy policy filters] to support different security or privacy policies.
Access Control	AC-04(12)	Data Type Identifiers	When transferring information between different security domains, use CMS-defined data type identifiers (defined in applicable security/privacy plans) to validate data essential for information flow decisions.
Access Control	AC-04(13)	Decomposition Into Policy-Relevant Subcomponents	When transferring information between different security domains, decompose information into [CMS-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.
Access Control	AC-04(14)	Security or Privacy Policy Filter Constraints	When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] requiring fully enumerated formats that
Access Control	AC-04(15)	Detection of Unsanctioned Information	When transferring information between different security domains, examine the information for the presence of unsanctioned information and prohibit the transfer of such information in accordance with the applicable CMS security or privacy policy.
Access Control	AC-04(17)	Domain Authentication	Uniquely identify and authenticate source and destination points by organization, system, application, service, and/or individual for information transfer.
Access Control	AC-04(19)	Validation of Metadata	When transferring information between different security domains, implement [CMS-defined security or privacy policy filters] on metadata
Access Control	AC-04(20)	Approved Solutions	Employ [CMS-defined solutions in approved configurations] to control the flow of CMS-defined information] across security domains.
Access Control	AC-04(21)	Physical or Logical Separation of Information Flows	Separate information flows logically or physically using [CMS-defined mechanisms and/or techniques] to accomplish [CMS-defined required separations by types of information].
Access Control	AC-04(22)	Access Only	Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing information flow between the different security domains.
Access Control	AC-04(23)	Modify Non-Releasable Information	When transferring information between different security domains, modify non-releasable information by implementing defined modification action (defined in applicable security and
Access Control	AC-04(24)	Internal Normalized Format	When transferring information between different security domains, parse incoming data into an
Access Control	AC-04(25)	Data Sanitization	When transferring information between different security domains, sanitize data to minimize delivery of malicious content, command and control of malicious code, malicious code augmentation, and steganography encoded data, and spillage of sensitive information in accordance with the latest revision of NIST SP 800-88, Guidelines for Media Sanitization, and
Access Control	AC-04(26)	Audit Filtering Actions	When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered.
Access Control	AC-04(27)	Redundant/Independent Filtering Mechanisms	When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.
Access Control	AC-04(28)	Linear Filter Pipelines	When transferring information between different security domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.
Access Control	AC-04(29)	Filter Orchestration Engines	When transferring information between different security domains, employ content filter orchestration engines to ensure that: (a) Content filtering mechanisms successfully complete execution without errors; and (b) Content filtering actions occur in the correct order and comply with CMS-defined policy.
Access Control	AC-04(30)	Filter Mechanisms Using	When transferring information between different security domains, implement content filtering
Access Control	AC-04(31)	Failed Content Transfer	When transferring information between different security domains, prevent the transfer of failed
Access Control	AC-04(32)	Process Requirements for Information Transfer	When transferring information between different security domains, the process that transfers information between filter pipelines: (a) Does not filter message content; (b) Validates filtering metadata; (c) Ensures the content associated with the filtering metadata has successfully completed filtering; and
Access Control	AC-06(04)	Separate Processing Domains	Provide separate processing domains to enable finer-grained allocation of user privileges.
Access Control	AC-07(03)	Biometric Attempt Limiting	Limit the number of unsuccessful biometric logon attempts to three (3).
Access Control	AC-07(04)	Use of Alternate Authentication Factor	(a) Allow the use of CMS-defined authentication factors that are different from the primary authentication factors after the number of organization-defined consecutive invalid logon attempts have been exceeded; and (b) Enforce a limit of consecutive invalid logon attempts as specified in Implementation Standard 1 through use of the alternative factors by a user during the time period specified in Implementation Standard 1.
Access Control	AC--09(02)	Successful and Unsuccessful Logons	Notify the user, upon successful logon, of the number of [Selection: successful logons; unsuccessful logon attempts; both] during [CMS-defined time period].
Access Control	AC-09(03)	Notification of Account Changes	Notify the user, upon successful logon, of changes to [CMS-defined security-related characteristics or parameters of the user's account] during [CMS-defined time
Access Control	AC-09(04)	Additional Logon Information	Notify the user, upon successful logon, of the following additional information: [CMS-defined additional information].
Access Control	AC-12(01)	User-Initiated Logouts	Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [CMS-defined information
Access Control	AC-12(02)	Termination Message	Display an explicit logout message to users indicating the termination of authenticated communications sessions.
Access Control	AC-12(03)	Timeout Warning Message	Display an explicit message to users indicating that the session will end in defined time until end
Access Control	AC-16	Security and Privacy Attributes	(a) Provide the means to associate CCIC-defined security and privacy attributes with defined security and privacy attribute values for information in storage, in process, and/or in transmission; (b) Ensure that the attribute associations are made and retained with the information; (c) Establish the permitted CCIC-defined security and privacy attributes for all CMS systems from the attributes defined in AC-16a ; (d) Determine the permitted CCIC-defined attribute values or ranges for each of the established attributes; (e) Audit changes to attributes; and (f) Review CCIC-defined security and privacy attributes for applicability no less often than annually.
Access Control	AC-16(01)	Dynamic Attribute Association	Dynamically associate security and privacy attributes with [CMS-defined subjects and objects] in accordance with the following security and privacy policies as information is created and combined: [CMS-defined security and privacy policies].
Access Control	AC-16(02)	Attribute Value Changes by	Provide authorized individuals (or processes acting on behalf of individuals) the capability
Access Control	AC-16(03)	Maintenance of Attribute Associations by System	Maintain the association and integrity of defined security and privacy attributes (defined in applicable security/privacy plans) to defined subjects and objects (defined in applicable
Access Control	AC-16(04)	Association of Attributes by Authorized Individuals	Provide the capability to associate [CMS-defined security and privacy attributes] with [CMS-defined subjects and objects] by authorized individuals (or processes acting on behalf of
Access Control	AC-16(05)	Attribute Displays on Objects	Display security and privacy attributes in human-readable form on each object that the system
Access Control	AC-16(06)	Maintenance of Attribute	Require personnel to associate and maintain the association of [CMS-defined security and
Access Control	AC-16(07)	Consistent Attribute Interpretation	Provide a consistent interpretation of security and privacy attributes transmitted between distributed system components.
Access Control	AC-16(08)	Association Techniques and Technologies	Implement [CMS-defined techniques and technologies] in associating security and privacy attributes to information.
Access Control	AC-16(09)	Attribute Reassignment-Regrading Mechanisms	Change security and privacy attributes associated with information only via regrading mechanisms validated using [CMS-defined techniques or procedures].
Access Control	AC-16(10)	Attribute Configuration by Authorized Individuals	Provide authorized individuals the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects.
Access Control	AC-17(10)	Authenticate Remote Commands	Implement defined mechanisms (specified in applicable security and privacy plan) to authenticate defined remote commands (specified in applicable security and privacy plan).
Access Control	AC-19(04)	Restrictions for Classified Information	(a) Prohibit the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and (b) Enforce the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information: (1) Connection of unclassified mobile devices to classified systems is prohibited; (2) Connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official; (3) Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and (4) Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [CMS-defined security officials], and if classified information is found, the incident handling policy is followed. (c) Restrict the connection of classified mobile devices to classified systems in accordance
Access Control	AC-20(04)	Network Accessible Storage	Prohibit the use of [CMS-defined network accessible storage devices] in external systems.
Access Control	AC-21(01)	Automated Decision Support	
Access Control	AC-21(02)	Information Search and	
Access Control	AC-23	Data Mining Protection	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.
Access Control	AC-24	Access Control Decisions	[Selection: Establish procedures; Implement mechanisms] to ensure [CMS-defined access control decisions] are applied to each access request prior to access enforcement.
Access Control	AC-24(01)	Transmit Access	Transmit [CMS-defined access authorization information] using
Access Control	AC-24(02)	No User or Process Identity	Enforce access control decisions based on [CMS-defined security or privacy attributes] that do not include the identity of the user or process acting on behalf of the user.
Access Control	AC-25	Reference Monitor	Implement a reference monitor for [CMS-defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.
Awareness and Training	AT-06	Training Feedback	Provide feedback on organizational training results CMS Training teams on a monthly basis.
Audit and Accountability	AU-04(01)	Transfer to Alternate Storage	Transfer audit logs[CMS-defined frequency]to a different system, system component, or media other than the system or system component conducting the logging.
Audit and Accountability	AU-05(03)	Configurable Traffic Volume Thresholds	Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and reject; delay network traffic above those thresholds.
Audit and Accountability	AU-05(04)	Shutdown on Failure	Invoke a full system shutdown; partial system shutdown; degraded operational mode with limited mission or business functionality available in the event of CMS-defined audit logging failures], unless an alternate audit logging capability exists.
Audit and Accountability	AU-05(05)	Alternate Audit Logging Capability	Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that implements alternate audit logging functionality (defined in applicable system security and privacy plan).
Audit and	AU-06(04)	Central Review and Analysis	Provide and implement the capability to centrally review and analyze audit records from multiple
Audit and Accountability	AU-06(07)	Permitted Actions	Specify the permitted actions for each (one or more): system process; role; user associated with the review, analysis, and reporting of audit record information.
Audit and Accountability	AU-06(08)	Full Text Analysis of Privileged Commands	Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.
Audit and Accountability	AU-06(09)	Correlation with Information from Nontechnical Sources	Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.
Audit and Accountability	AU-09(01)	Hardware Write-Once Media	Write audit trails to hardware-enforced, write-once media.
Audit and Accountability	AU-09(07)	Store on Component with Different Operating System	Store audit information on a component running a different operating system than the system or component being audited.
Audit and Accountability	AU-10(01)	Association of Identities	(a) Bind the identity of the information producer with the information to defined strength of binding (defined in applicable system security and privacy plan); and (b) Provide the means for authorized individuals to determine the identity of the producer of the information
Audit and Accountability	AU-10(02)	Validate Binding of Information Producer Identity	(a) Validate the binding of the information producer identity to the information at CMS-defined frequency and (b) Perform CMS-defined actions in the event of a validation error
Audit and Accountability	AU-10(03)	Chain of Custody	Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.
Audit and Accountability	AU-10(04)	Validate Binding of Information Reviewer Identity	(a) Validate the binding of the information reviewer identity to the information at the transfer or release points prior to release or transfer between CMS-defined security domains; and (b) Perform CMS-defined actions in the event of a validation error.
Audit and Accountability	AU-11(01)	Long-Term Retrieval Capability	Employ CMS-defined measures to ensure that long-term audit records generated by the system can be retrieved.
Audit and Accountability	AU-12(02)	Standardized Formats	Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.
Audit and Accountability	AU-12(04)	Query Parameter Audits of Personally Identifiable Information	Provide and implement the capability for auditing the parameters of user query events for data sets containing personally identifiable information.
Audit and Accountability	AU-13	Monitoring of Information Disclosure	a. Monitor open-source information and/or information sites for evidence of unauthorized disclosure of organizational information (defined in applicable system security and privacy plan); and b. If an information disclosure is discovered: 1. Notify CMS-defined personnel or roles; (such as Incident Response Team CCIC IMT) and 2. Take the following additional actions: (Follow the incident and breach response process as defined in applicable system security and privacy plan).
Audit and	AU-13(01)	Use of Automated Tools	Monitor open-source information and information sites using CMS-defined automated
Audit and Accountability	AU-13(02)	Review of Monitored Sites	Review the list of open-source information sites being monitored CMS-defined frequency].
Audit and Accountability	AU-13(03)	Unauthorized Replication of Information	Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.

Audit and Accountability	AU-14	Session Audit	a. Provide and implement the capability for CMS-defined users or roles] to(one or more): record; view; hear; log]the content of a user session under CMS-defined circumstances]; and b. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
Audit and Accountability	AU14-(01)	System Start-Up	Initiate session audits automatically at system start-up
Audit and	AU-14(03)	Remote Viewing and	Provide and implement the capability for authorized users to remotely view and hear
Audit and	AU-16(01)	Identity Preservation	Preserve the identity of individuals in cross-organizational audit trails
Audit and Accountability	AU-16(02)	Sharing of Audit Information	Provide cross-organizational audit information to CMS-defined organizations based on defined cross-organizational sharing agreements (defined in the applicable system security and privacy plan).
Audit and Accountability	AU-16(03)	Disassociability	Implement measures (defined in the applicable system security and privacy plan)to disassociate individuals from audit information transmitted across organizational boundaries.
Assessment, Authorization, and Monitoring	CA-03(06)	Transfer Authorizations	Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.
Assessment, Authorization, and Monitoring	CA-03(07)	Transitive Information Exchanges	(a) Identify transitive (downstream) information exchanges with other systems through the systems identified in CA-3a; and (b) Take measures to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive (downstream) systems cannot be verified or validated.
Assessment, Authorization, and Monitoring	CA-05(01)	Automation Support for Accuracy and Currency	Ensure the accuracy, currency, and availability of the plan of action and milestones (POA&M) for the system using CMS-defined automated mechanisms.
Assessment, Authorization, and Monitoring	CA-06(02)	Joint Authorization Inter-Organization	Employ a joint authorization process for the system that includes multiple authorizing officials with at least one authorizing official from an organization external to the organization conducting the authorization.
Assessment, Authorization, and Monitoring	CA-07(05)	Consistency Analysis	Employ actions to validate that policies are established and implemented controls are operating in a consistent manner.
Assessment, Authorization, and Monitoring	CA-07(06)	AUTOMATION SUPPORT FOR MONITORING	Ensure the accuracy, currency, and availability of monitoring results for the system using [CMS-defined automated mechanisms].
Configuration Management	CM-03(03)	Automated Change Implementation	Implement changes to the current system baseline and deploy the updated baseline across the installed base using [Assignment: organization-defined automated mechanisms].
Configuration Management	CM-03(05)	Automated Security Response	Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner: CMS-defined security responses.
Configuration Management	CM-03(08)	Prevent or Restrict Configuration Changes	Prevent or restrict changes to the configuration of the system when the changes do not meet the system's mission or operational requirements, and the security and privacy functionality of the
Configuration Management	CM-05(04)	Dual Authorization	Enforce dual authorization for implementing changes to CMS-defined system components and system-level information.
Configuration	CM-07(03)	Registration Compliance	Ensure compliance with CMS-defined registration requirements for
Configuration Management	CM-07(04)	Unauthorized Software - Deny	Per NIST SP 800-53r5, when software allow listing (CM-7(5), Authorized Software - Allow has been implemented for systems with a FIPS 199 security categorization of Moderate, this control enhancement is not required. If software allow listing (CM-7(5)) is not implemented, the organization: (a) Identify software programs (defined in the applicable security and privacy plan) not authorized to execute on the information system; (b) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and (c) Review and update the list of unauthorized software programs no less often than every seventy-two (72) hours
Configuration Management	CM-07(06)	Confined Environments with Limited Privileges	Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges (defined in applicable system security and privacy plan)
Configuration Management	CM-07(07)	Code Execution in Protected Environments	Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of defined personnel or roles [e.g., Authorizing Official] (specified in applicable system security and privacy plan) when such code is: (a) Obtained from sources with limited or no warranty; and/or (b) Without the provision of source code.
Configuration Management	CM-07(08)	Binary or Machine Executable Code	(a) Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; and (b) Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.
Configuration Management	CM-08(08)	Automated Location Tracking	Support the tracking of system components by geographic location using CMS-defined automated mechanisms].
Configuration Management	CM-08(09)	Assignment of Components to Systems	(a) Assign system components to a system; and (b) Receive an acknowledgement from [Assignment: organization-defined personnel or
Configuration Management	CM-10(01)	Open Source Software	Establish the following restrictions on the use of open-source software: CMS-defined restrictions].
Configuration Management	CM-11(03)	Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using CMS-defined automated mechanisms.
Configuration Management	CM-13	Data Action Mapping	Develop and document a map of system data actions.
Contingency Planning	CP-04(03)	Automated Testing	Automated mechanisms facilitate thorough and effective testing of contingency plans by providing more complete coverage of contingency issues, selecting more realistic test scenarios and environments, and effectively stressing the system and supported mission
Contingency Planning	CP-04(05)	Self-Challenge	Employ CMS-defined mechanisms to CMS defined system or system component to disrupt and adversely affect the system or system component.
Contingency Planning	CP-07(06)	Inability to Return to Primary Site	Plan and prepare for circumstances that preclude returning to the primary processing site.
Contingency Planning	CP-09(06)	Redundant Secondary System	Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.
Contingency Planning	CP-09(07)	Dual Authorization	Enforce dual authorization for the deletion or destruction of CMS-defined backup information].
Identification and	IA-02(10)	SINGLE SIGN-ON	Provide a single sign-on capability for CMS-defined system accounts and services
Identification and	IA-02(13)	OUT-OF-BAND	Implement out-of-band authentication mechanisms under defined conditions (specified in
Identification and Authentication	IA-03(01)	CRYPTOGRAPHIC BIDIRECTIONAL	Authenticate CMS-defined devices and/or types of devices]before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is
Identification and Authentication	IA-03(03)	DYNAMIC ADDRESS ALLOCATION	(a) Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with CMS-defined lease information and lease duration; and
Identification and	IA-03(04)	DEVICE ATTESTATION	Handle device identification and authentication based on attestation by CMS-defined
Identification and Authentication	IA-04(01)	PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC	Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts.
Identification and	IA-04(05)	DYNAMIC MANAGEMENT	Manage individual identifiers dynamically in accordance with CMS-defined dynamic identifier
Identification and	IA-04(06)	CROSS-ORGANIZATION	Coordinate with the following external organizations for cross-organization management of
Identification and Authentication	IA-04(08)	PAIRWISE PSEUDONYMOUS	Generate pairwise pseudonymous identifiers.
Identification and	IA-04(09)	ATTRIBUTE	Maintain the attributes for each uniquely identified individual, device, or service in CMS-defined
Identification and Authentication	IA-05(05)	CHANGE AUTHENTICATORS	Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.
Identification and Authentication	IA-05(07)	NO EMBEDDED UNENCRYPTED STATIC	Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.
Identification and	IA-05(08)	MULTIPLE SYSTEM	Implement CMS-defined security controls to manage the risk of compromise due to individuals
Identification and	IA-05(09)	FEDERATED	Use the following external organizations to federate credentials: CMS-defined external
Identification and	IA-05(10)	DYNAMIC CREDENTIAL	Bind identities and authenticators dynamically using the following rules: CMS-defined binding
Identification and Authentication	IA-05(12)	BIOMETRIC AUTHENTICATION	For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements CMS-defined biometric quality requirements.
Identification and	IA-05(13)	EXPIRATION OF CACHED	Prohibit the use of cached authenticators after CMS-defined time period.
Identification and Authentication	IA-05(14)	MANAGING CONTENT OF PKI TRUST STORES	For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems,
Identification and Authentication	IA-05(16)	IN-PERSON OR TRUSTED EXTERNAL PARTY	Require that the issuance of CMS-defined types of and/or specific authenticators be conducted [Selection: in person; by a trusted external party] before CMS-defined registration authority with
Identification and Authentication	IA-05(17)	PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS	Employ presentation attack detection mechanisms for biometric-based authentication.
Identification and Authentication	IA-05(18)	PASSWORD MANAGERS	(a) Employ CMS-defined password managers to generate and manage passwords; and (b) Protect the passwords using CMS-defined controls.
Identification and	IA-08(05)	ACCEPTANCE OF PIV-I	Accept and verify federated or PKI credentials that meet CMS-defined policy.
Identification and Authentication	IA-08(06)	DISASSOCIABILITY	Implement the following measures to disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties: CMS-defined
Identification and	IA-09	SERVICE IDENTIFICATION	Uniquely identify and authenticate CMS-defined system services and applications before
Identification and	IA-10	ADAPTIVE	Require individuals accessing the system to employ CMS-defined supplemental authentication
Identification and	IA-12(01)	SUPERVISOR	Require that the registration process to receive an account for logical access includes
Identification and Authentication	IA-12(06)	ACCEPT EXTERNALLY-PROOFED IDENTITIES	Accept externally-proofed identities at CMS-defined identity assurance level.
Incident Response	IR-03(01)	Automated Testing	Test the incident response capability using automated mechanisms.
Incident Response	IR-03(03)	Continuous Improvement	Use qualitative and quantitative data from testing to: (a) Determine the effectiveness of incident response processes; (b) Continuously improve incident response processes; and (c) Provide incident response measures and metrics that are accurate, consistent, and in a
Incident Response	IR-04(03)	Continuity of Operations	Identify classes of incidents and take the following appropriate actions (defined in applicable system's Incident Response Plan) in response to those incidents to ensure continuation of CMS missions and business functions. Classes of incident are based on attack vector (e.g., attack via external media, the web, improper system use, loss of equipment) and serve to further define specific handling procedures: o Graceful degradation o Information system shutdown o Fall back to manual mode/alternative technology whereby the system operates differently o Employing deceptive measures o Alternate information flows, or
Incident Response	IR-04(05)	AUTOMATIC DISABLING OF SYSTEM	Implement a configurable capability to automatically disable the system if [CMS-defined security violations] are detected.
Incident Response	IR-04(07)	Insider Threats – Intra-Organization Coordination	Coordinate an incident handling capability for insider threats across the CMS enterprise through CMS Counterintelligence and Insider Threat Program that include following organizational entities: o Mission/Business Owners o Information System Owners (ISO) o Office of Human Capital (OHC) o Office of Acquisitions and Grant Management (OAGM) o Personnel/Physical Security Offices (OSSO)
Incident Response	IR-04(09)	DYNAMIC RESPONSE	Employ[CMS-defined dynamic response capabilities] to respond to incidents
Incident Response	IR-04(12)	Malicious Code and Forensic Analysis	Analyze malicious code and/or other residual artifacts remaining in the system after the incident.
Incident Response	IR-04(13)	Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [CMS-defined environments or resources].
Incident Response	IR-04(15)	Publication Relations and Reputation Repair	(a) Manage public relations associated with an incident; and (b) Employ measures to repair the reputation of the organization.
Incident Response	IR-06(02)	VULNERABILITIES	Report system vulnerabilities associated with reported incidents to [CMS-defined personnel or
Incident Response	IR-07(02)	Coordination with External Providers	(a) Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and (b) Identify organizational incident response team members to the external providers.
Incident Response	IR-09	Information Spillage Response	Respond to information spills by: (a). Assigning applicable CMS Information System Security Officer (ISSO) with responsibility for responding to information spills; (b). Identifying the specific information involved in the system contamination; (c). Alerting the CCIC IMT of the information spill using a method of communication not associated with the spill (e.g. by calling CMS IT Service Desk); d. Isolating the contaminated system or system component; e. Eradicating the information from the contaminated system or component; f. Identifying other systems or system components that may have been subsequently contaminated; and g. Performing additional response actions as directed by the CCIC IMT and any other response actions defined in the system incident response plan. .
Incident Response	IR-09(02)	Training	Provide information spillage response training no less often than annually [every three hundred and sixty-five (365) days].
Incident Response	IR-09(03)	Post-Spill Operations	Implement procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.
Incident Response	IR-09(04)	Exposure to Unauthorized Personnel	Employ CMS rules of behavior and defined security and privacy safeguards to address the risk for personnel exposed to information not within assigned access authorizations.
Maintenance	MA-04(01)	Logging and Review	(a) Log audit events for nonlocal maintenance and diagnostic sessions; and (b) Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.
Maintenance	MA-04(04)	Authentication and Separation of Maintenance Sessions	(a) Employing authenticators that are replay resistant; and (b) Separating the maintenance sessions from other network sessions with the system by either: (1) Physically separated communications paths; or
Maintenance	MA-04(05)	Approvals and Notifications	(a) Require the approval of each nonlocal maintenance session by applicable personnel or roles; and (b) Notify the following personnel or roles of the date and time of planned nonlocal maintenance:
Maintenance	MA-04(06)	Cryptographic Protection	Implements the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: e.g. the use of FIPS-validated cryptography.
Maintenance	MA-04(07)	Disconnect Verification	Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.
Maintenance	MA-05(04)	Foreign Nationals	Ensure that: (a) Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and (b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully
Maintenance	MA-05(05)	Non-System Maintenance	Ensure that non-escorted personnel performing maintenance activities not directly associated
Maintenance	MA-06(01)	Preventive Maintenance	Perform preventive maintenance on system components at the applicable RTO specified in the contingency plan.
Maintenance	MA-06(02)	Predictive Maintenance	Perform predictive maintenance on system components at the applicable RTO specified in the contingency plan.
Maintenance	MA-06(03)	Automated Support for Predictive Maintenance	Transfer predictive maintenance data to a maintenance management system using automated mechanisms defined in applicable system security and privacy plan.
Maintenance	MA-07	Field Maintenance	Restrict or prohibits field maintenance on systems or system components to trusted maintenance facilities.
Media Protection	MP-04(02)	Automated Restricted Access	Restrict access to media storage areas and log access attempts and access granted using CMS automated mechanisms (defined in system security and privacy plan).
Media Protection	MP-06(07)	Dual Authorization	Enforce dual authorization for the sanitization of digital and non-digital system media.
Media Protection	MP-08	Media Downgrading	a. Establish system media downgrading process that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information; b. Verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information; c. Identify system media requiring downgrading; and d. Downgrade the identified system media using the established process.
Media Protection	MP-08(01)	Documentation of Process	Document system media downgrading actions.
Media Protection	MP-08(02)	Equipment Testing	Test downgrading equipment and procedures within every three hundred sixty-five days (365)
Media Protection	MP-08(03)	Controlled Unclassified Information	Downgrade system media containing controlled unclassified information (CUI) prior to public release in accordance with applicable federal and organizational standards and policies.
Media Protection	MP-08(04)	Classified Information	Downgrade system media containing classified information prior to release to individuals without required access authorizations.
Physical and Environmental Protection	PE-02(02)	Two Forms of Identification	Require two forms of identification from the following forms of identification for visitor access to the facility where the system resides: CMS-defined list of acceptable forms of identification.
Physical and Environmental Protection	PE-02(03)	Restrict Unescorted Access	Restrict unescorted access to the facility where the system resides to personnel with one or more: security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information
Physical and Environmental	PE-03(02)	Facility and Systems	Perform security checks CMS-defined frequency at the physical perimeter of the facility or system for exfiltration of information or removal of system components.
Physical and Environmental	PE-03(03)	Continuous Guards	Employ guards to control CMS-defined physical access points to the facility where the system resides 24 hours per day, 7 days per week.
Physical and Environmental Protection	PE-03(04)	Lockable Casings	Use lockable physical casings to protect CMS-defined system components] from unauthorized physical access
Physical and Environmental Protection	PE-03(05)	Tamper Protection	Employ CMS-defined anti-tamper technologies to detect; prevent physical tampering or alteration of CMS-defined hardware components within the system.
Physical and Environmental	PE-03(07)	Physical Barriers	Limit access using physical barriers.
Physical and Environmental Protection	PE-03(08)	Access Control Vestibules	Employ access control vestibules at defined locations within the facility (defined in the applicable security and privacy plan).
Physical and Environmental Protection	PE-05(02)	Link to Individual Identity	Link individual identity to receipt of output from output devices.
Physical and Environmental Protection	PE-06(02)	Automated Intrusion Recognition and Responses	Recognize CMS-defined classes or types of intrusions] and initiate CMS-defined response actions] using CMS-defined automated mechanisms].
Physical and Environmental Protection	PE-06(03)	Video Surveillance	(a) Employ video surveillance of CMS-defined operational areas; (b) Review video recordings CMS-defined frequency; and (c) Retain video recordings for CMS-defined time period.
Physical and Environmental Protection	PE-08(03)	Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: 1. Name and organization of the person visiting; 2. Visitor's signature; 3. Form of identification;
Physical and Environmental	PE-09(01)	Redundant Cabling	Employ redundant power cabling paths that are physically separated by CMS-defined distance.
Physical and Environmental	PE-09(02)	Automatic Voltage Controls	Employ automatic voltage controls for CMS-defined critical system components.
Physical and Environmental Protection	PE-11(02)	Alternate Power Supply – Self-Contained	Provide an alternate power supply for the system that is activated manually; automatically and that is: (a) Self-contained; (b) Not reliant on external power generation; and (c) Capable of maintaining [Selection: minimally required operational capability; full
Physical and Environmental	PE-14(01)	Automatic Controls	Employ the following automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system: CMS-defined automatic environmental controls.
Physical and Environmental Protection	PE-14(02)	Monitoring with Alarms and Notifications	Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to [Assignment: organization defined personnel or roles].
Physical and Environmental Protection	PE-19	Information Leakage	: Protect the system from information leakage due to electromagnetic signals emanations.
Physical and Environmental	PE-19(01)	National Emissions Policies and Procedures	Protect system components, associated data communications, and networks in accordance with national Emissions Security policies and procedures based on the security category or
Physical and Environmental Protection	PE-20	Asset Monitoring and Tracking	Employ CMS-defined asset location technologies to track and monitor the location and movement of CMS-defined assets] within CMS-defined controlled areas].
Physical and Environmental Protection	PE-21	Electromagnetic Pulse Protection	Employ defined protective measures (defined in the applicable security and privacy plan) against electromagnetic pulse damage for systems and system components.
Physical and Environmental Protection	PE-22	Component Marking	Mark system hardware components (defined in the applicable security and privacy plan) indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.
Physical and Environmental Protection	PE-23	Facility Location	(a) Plan the location or site of the facility where the system resides considering physical and environmental hazards; and (b) For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.

Planning	PL-08(02)	Supplier Diversity	Require that CMS-defined controls (defined in applicable security/privacy plans) allocated to locations and architectural layers (defined in applicable security/privacy plans) are obtained from different suppliers.	Require that CMS-defined controls (defined in applicable security/privacy plans) allocated to locations and architectural layers (defined in applicable security/privacy plans) are obtained from different suppliers.		System
Personnel Security	PS-03(01)	Classified Information	Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.	Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.		System
Personnel Security	PS-03(02)	Formal Indoctrination	Verify that individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.	Verify that individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.	**High, Moderate & Low:** **Std.1.** Ensure individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination, are formally indoctrinated for all the	System
Personnel Security	PS-03(03)	Information Requiring Special Protective Measures	Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection: a. Have valid access authorizations that are demonstrated by assigned official government duties; and b. Satisfy additional personnel screening criteria consistent with the sensitivity of the information being accessed.	~~The organization ensures~~Verify that individuals accessing ~~an information~~ system processing, storing, or transmitting information requiring special protection:¶a. Have valid access authorizations that are demonstrated by assigned official government duties; and¶b. Satisfy additional personnel screening ~~periodically~~ criteria consistent with the sensitivity of the information being accessed.	**High, Moderate & Low:** **Std.1** - Coordinate with appropriate CMS CIO POCs and HHS Office of Security and Strategic Information (OSSI) POCs to ensure background checks are conducted on all individuals identified by system owners with access to CMS information systems in accordance with position sensitivity designation as derived by the use of the appropriate CMS tool.	System
Personnel Security	PS-06(02)	Classified Information Requiring Special Protection	Verify that access to classified information requiring special protection is granted only to individuals who: a. Have a valid access authorization that is demonstrated by assigned official government duties; b. Satisfy associated personnel security criteria; and	Verify that access to classified information requiring special protection is granted only to individuals who:¶a. Have a valid access authorization that is demonstrated by assigned official government duties;¶b. Satisfy associated personnel security criteria; and¶c. Have read, understood, and signed a nondisclosure agreement.		System
Personnel Security	PS-06(03)	Post-Employment Requirements	a. Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and b. Require individuals to sign an acknowledgment of these requirements, if applicable, as part of	a. Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and¶b. Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.		System
Personally Identifiable Information Processing and Transparency	PT-02(01)	Data Tagging	Systems processing, storing, or transmitting PII (to include PHI): Attach data tags containing [CMS Entity-Defined: Mission/Business/System]-defined permitted processing indicators (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans) to [CMS Entity-Defined: Mission/Business/System]-defined elements (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans) of	Systems processing, storing, or transmitting PII (to include PHI):¶Attach data tags containing [CMS Entity-Defined: Mission/Business/System]-defined permitted processing indicators (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans) to [CMS Entity-Defined: Mission/Business/System]-defined elements (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans) of personally identifiable information.		System
Personally Identifiable Information Processing and	PT-02(02)	Automation	Systems processing, storing, or transmitting PII (to include PHI): Manage enforcement of the authorized processing of personally identifiable information using CMS Mission/Business/System-defined automated mechanisms (defined in applicable [CMS	Systems processing, storing, or transmitting PII (to include PHI):¶Manage enforcement of the authorized processing of personally identifiable information using CMS Mission/Business/System-defined automated mechanisms (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans).		System
Personally Identifiable Information Processing and Transparency	PT-03(01)	Data Tagging	Systems processing, storing, or transmitting PII (to include PHI): Attach data tags containing the following purposes to [CMS Entity-Defined: Mission/Business/System]-defined elements of personally identifiable information (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans): [CMS Entity-Defined: Mission/Business/System]-defined processing purposes.	Systems processing, storing, or transmitting PII (to include PHI):¶Attach data tags containing the following purposes to [CMS Entity-Defined: Mission/Business/System]-defined elements of personally identifiable information (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans): [CMS Entity-Defined: Mission/Business/System]-defined processing purposes.		System
Personally Identifiable Information Processing and	PT-03(02)	Automation	Systems processing, storing, or transmitting PII (to include PHI): Track processing purposes of personally identifiable information using CMS Mission/Business/System-defined automated mechanisms (defined in applicable [CMS Entity-	Systems processing, storing, or transmitting PII (to include PHI):¶Track processing purposes of personally identifiable information using CMS Mission/Business/System-defined automated mechanisms (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans).		System
Personally Identifiable Information Processing and Transparency	PT-04(01)	Tailored Consent	Systems processing, storing, or transmitting PII (to include PHI): Provide [CMS Entity-Defined: Mission/Business/System]-defined mechanisms (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans) to allow individuals to tailor processing permissions to selected elements of personally identifiable information.	Systems processing, storing, or transmitting PII (to include PHI):¶Provide [CMS Entity-Defined: Mission/Business/System]-defined mechanisms (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans) to allow individuals to tailor processing permissions to selected elements of personally identifiable information.		System
Personally Identifiable Information Processing and Transparency	PT-04(02)	Just-in-time Consent	Systems processing, storing, or transmitting PII (to include PHI): Present [CMS Entity-Defined: Mission/Business/System]-defined consent mechanisms (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans) to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action.	Systems processing, storing, or transmitting PII (to include PHI):¶Present [CMS Entity-Defined: Mission/Business/System]-defined consent mechanisms (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans) to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action.		System
Personally Identifiable Information Processing and	PT-04(03)	Revocation	Implement CMS-defined tools or mechanisms for individuals to revoke consent to the processing of their personally identifiable information.	Implement CMS-defined tools or mechanisms for individuals to revoke consent to the processing of their personally identifiable information.		System
Personally Identifiable Information Processing and Transparency	PT-05(01)	Just-in-time Notice	Systems processing, storing, or transmitting PII (to include PHI): Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or [CMS Entity-Defined: Mission/Business/System]-defined frequency (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans).	Systems processing, storing, or transmitting PII (to include PHI):¶Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or [CMS Entity-Defined: Mission/Business/System]-defined frequency (defined in applicable [CMS Entity-Defined: Mission/Business/System] security/privacy plans).		System
Risk Assessment	RA-02(01)	Impact-Level Prioritization	Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.	Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.		System
Risk Assessment	RA-03(02)	Use of All-Source Intelligence	Use all-source intelligence to assist in the analysis of risk.	Use all-source intelligence to assist in the analysis of risk.		System
Risk Assessment	RA-03(03)	Dynamic Threat Awareness	Determine the current cyber threat environment on an ongoing basis using CMS-defined means.	Determine the current cyber threat environment on an ongoing basis using CMS-defined means.		System
Risk Assessment	RA-03(04)	Predictive Cyber Analytics	Employ advanced automation and analytics capabilities to predict and identify risks to systems or system components.	Employ advanced automation and analytics capabilities to predict and identify risks to systems or system components.		System
Risk Assessment	RA-05(03)	Breadth and Depth of Coverage	Define the breadth and depth of vulnerability scanning coverage.	~~The organization employs vulnerability scanning procedures that can identify/demonstrate~~Define the breadth and depth of vulnerability scanning coverage ~~(i.e., information system components scanned and vulnerabilities checked)~~.		System
Risk Assessment	RA-05(08)	REVIEW HISTORIC AUDIT	Reviews historic audit logs to determine if a vulnerability identified in an CMS-defined system	Reviews historic audit logs to determine if a vulnerability identified in an CMS-defined system		System
Risk Assessment	RA-06	TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY	Employs a technical surveillance countermeasures survey at CMS-defined locations: at an CMS-defined frequency; when the following events or indicators occur: CMS-defined events or indicators.	Employs a technical surveillance countermeasures survey at CMS-defined locations: at an CMS-defined frequency; when the following events or indicators occur: CMS-defined events or indicators.		System
System and Services Acquisition	SA-04(03)	DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES	Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes: (a) [Assignment: organization-defined systems engineering methods]; (b) [Assignment: organization-defined [Selection (one or more): systems security; privacy] engineering methods]; and (c) [Assignment: organization-defined software development methods; testing, evaluation,	Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes:¶(a) [Assignment: organization-defined systems engineering methods];¶(b) [Assignment: organization-defined [Selection (one or more): systems security; privacy] engineering methods]; and¶(c) [Assignment: organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes].		System
System and Services Acquisition	SA-04(06)	USE OF INFORMATION ASSURANCE PRODUCTS	(a) Employ only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and (b) Ensure that these products have been evaluated and/or validated by NSA or in accordance	(a) Employ only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and¶(b) Ensure that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved		System
System and Services Acquisition	SA-04(07)	NIAP-APPROVED PROTECTION PROFILES	(a) Limit the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and (b) Require, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to	(a) Limit the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and¶(b) Require, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the		System
System and Services Acquisition	SA-04(08)	Continuous Monitoring Plan for Controls	Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that contains the level of detail that meets CMS and Federal requirements (e.g., Continuous Diagnostics and Mitigation, ongoing authorization)	~~The organization requires~~Require the developer of the ~~information~~ system, system component, or ~~information~~ system service to produce a plan for ~~the~~ continuous monitoring of ~~security~~ control effectiveness that contains the level of detail that meets CMS and Federal requirements (e.g., Continuous Diagnostics and Mitigation, ongoing authorization).		System
System and Services Acquisition	SA-4(11)	SYSTEM OF RECORDS	Include Privacy Act requirements per the HHS Policy for Information Technology Procurements - Security And Privacy Language or CMS-defined Privacy Act requirements in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an	Include Privacy Act requirements per the HHS Policy for Information Technology Procurements - Security And Privacy Language or CMS-defined Privacy Act requirements in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an		System
System and Services Acquisition	SA-04(10)	DATA OWNERSHIP	(a) Include organizational data ownership requirements in the acquisition contract; and (b) Require contractors to have policies and procedures in place to remove all data from the	(a) Include organizational data ownership requirements in the acquisition contract; and¶(b) Require contractors to have policies and procedures in place to remove all data from the		System
System and	SA-08(01)	CLEAR ABSTRACTIONS	Implement the security design principle of clear abstractions.	Implement the security design principle of clear abstractions.		System
System and	SA-08(02)	LEAST COMMON	Implement the security design principle of least common mechanism in [Assignment:	Implement the security design principle of least common mechanism in [Assignment:		System
System and	SA-08(03)	MODULARITY AND	Implement the security design principles of modularity and layering in [Assignment: organization	Implement the security design principles of modularity and layering in [Assignment: organization		System
System and	SA-08(04)	PARTIALLY ORDERED	Implement the security design principle of partially ordered dependencies in [Assignment:	Implement the security design principle of partially ordered dependencies in [Assignment:		System
System and	SA-08(05)	EFFICIENTLY MEDIATED	Implement the security design principle of efficiently mediated access in [Assignment:	Implement the security design principle of efficiently mediated access in [Assignment:		System
System and	SA-08(06)	MINIMIZED SHARING	Implement the security design principle of minimized sharing in [Assignment: organization-	Implement the security design principle of minimized sharing in [Assignment: organization-		System
System and	SA-08(07)	REDUCED COMPLEXITY	Implement the security design principle of reduced complexity in [Assignment: organization-	Implement the security design principle of reduced complexity in [Assignment: organization-		System
System and	SA-08(08)	SECURE EVOLVABILITY	Implement the security design principle of secure evolvability in [Assignment: organization-	Implement the security design principle of secure evolvability in [Assignment: organization-		System
System and	SA-08(9)	TRUSTED COMPONENTS	Implement the security design principle of trusted components in [Assignment: organization-	Implement the security design principle of trusted components in [Assignment: organization-		System
System and	SA-08(10)	HIERARCHICAL TRUST	Implement the security design principle of hierarchical trust in [Assignment: organization-	Implement the security design principle of hierarchical trust in [Assignment: organization-		System
System and	SA-8(11)	INVERSE MODIFICATION	Implement the security design principle of inverse modification threshold in [Assignment:	Implement the security design principle of inverse modification threshold in [Assignment:		System
System and	SA-8(12)	HIERARCHICAL	Implement the security design principle of hierarchical protection in [Assignment: organization-	Implement the security design principle of hierarchical protection in [Assignment: organization-		System
System and	SA-8(13)	MINIMIZED SECURITY	Implement the security design principle of minimized security elements in [Assignment:	Implement the security design principle of minimized security elements in [Assignment:		System
System and	SA-8(14)	LEAST PRIVILEGE	Implement the security design principle of least privilege in [Assignment: organization-defined	Implement the security design principle of least privilege in [Assignment: organization-defined		System
System and	SA-8(15)	PREDICATE PERMISSION	Implement the security design principle of predicate permission in [Assignment: organization-	Implement the security design principle of predicate permission in [Assignment: organization-		System
System and	SA-8(16)	SELF-RELIANT	Implement the security design principle of self-reliant trustworthiness in [Assignment:	Implement the security design principle of self-reliant trustworthiness in [Assignment:		System
System and	SA-8(17)	SECURE DISTRIBUTED	Implement the security design principle of secure distributed composition in [Assignment:	Implement the security design principle of secure distributed composition in [Assignment:		System
System and Services Acquisition	SA-8(18)	TRUSTED COMMUNICATIONS	Implement the security design principle of trusted communications channels in [Assignment: organization-defined systems or system components].	Implement the security design principle of trusted communications channels in [Assignment: organization-defined systems or system components].		System
System and	SA-8(19)	CONTINUOUS	Implement the security design principle of continuous protection in [Assignment: organization-	Implement the security design principle of continuous protection in [Assignment: organization-		System
System and	SA-8(20)	SECURE METADATA	Implement the security design principle of secure metadata management in [Assignment:	Implement the security design principle of secure metadata management in [Assignment:		System
System and	SA-8(21)	SELF-ANALYSIS	Implement the security design principle of self-analysis in [Assignment: organization-defined	Implement the security design principle of self-analysis in [Assignment: organization-defined		System
System and	SA-8(22)	ACCOUNTABILITY AND	Implement the security design principle of accountability and traceability in [Assignment:	Implement the security design principle of accountability and traceability in [Assignment:		System
System and	SA-8(23)	SECURE DEFAULTS	Implement the security design principle of secure defaults in [Assignment: organization-defined	Implement the security design principle of secure defaults in [Assignment: organization-defined		System
System and	SA-8(24)	SECURE FAILURE AND	Implement the security design principle of secure failure and recovery in [Assignment:	Implement the security design principle of secure failure and recovery in [Assignment:		System
System and	SA-8(25)	ECONOMIC SECURITY	Implement the security design principle of economic security in [Assignment: organization-	Implement the security design principle of economic security in [Assignment: organization-		System
System and	SA-8(26)	PERFORMANCE	Implement the security design principle of performance security in [Assignment: organization-	Implement the security design principle of performance security in [Assignment: organization-		System
System and	SA-8(27)	HUMAN FACTORED	Implement the security design principle of human factored security in [Assignment: organization-	Implement the security design principle of human factored security in [Assignment: organization-		System
System and	SA-8(28)	ACCEPTABLE SECURITY	Implement the security design principle of acceptable security in [Assignment: organization-	Implement the security design principle of acceptable security in [Assignment: organization-		System
System and Services Acquisition	SA-8(29)	REPEATABLE AND DOCUMENTED	Implement the security design principle of repeatable and documented procedures in [Assignment: organization-defined systems or system components].	Implement the security design principle of repeatable and documented procedures in [Assignment: organization-defined systems or system components].		System
System and	SA-8(30)	PROCEDURAL RIGOR	Implement the security design principle of procedural rigor in [Assignment: organization-defined	Implement the security design principle of procedural rigor in [Assignment: organization-defined		System
System and	SA-8(31)	SECURE SYSTEM	Implement the security design principle of secure system modification in [Assignment:	Implement the security design principle of secure system modification in [Assignment:		System
System and	SA-8(32)	SUFFICIENT	Implement the security design principle of sufficient documentation in [Assignment: organization-	Implement the security design principle of sufficient documentation in [Assignment: organization-		System
System and Services Acquisition	SA-09(02)	Identification of Functions, Ports, Protocols, and Services	Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services as defined in the applicable system security plan.	~~The organization requires~~Require providers of the following external ~~information~~ system services, ~~as defined in the applicable System Security Plan,~~ to identify the functions, ports, protocols, and other services required for the use of such services. as defined in the applicable		System
System and Services Acquisition	SA-09(03)	ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust		System
System and Services Acquisition	SA-09(04)	CONSISTENT INTERESTS OF CONSUMERS AND	Take the following actions to verify that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests: [Assignment:	Take the following actions to verify that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests: [Assignment:		System
System and Services Acquisition	SA-09(06)	ORGANIZATION-CONTROLLED	Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.	Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.		System
System and Services Acquisition	SA-09(07)	ORGANIZATION-CONTROLLED INTEGRITY	Provide the capability to check the integrity of information while it resides in the external system.	Provide the capability to check the integrity of information while it resides in the external system.		System
System and Services Acquisition	SA-09(08)	PROCESSING AND STORAGE LOCATION —	Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.	Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.		System
System and Services Acquisition	SA-10(01)	Software and Firmware Integrity Verification	Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.	~~The organization requires~~Require the developer of the ~~information~~ system, system component, or ~~information~~ system service to enable integrity verification of software and firmware components.		System
System and Services Acquisition	SA-10(02)	ALTERNATIVE CONFIGURATION	Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.	Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.		System
System and	SA-10(03)	HARDWARE INTEGRITY	Require the developer of the system, system component, or system service to enable integrity	Require the developer of the system, system component, or system service to enable integrity		System
System and Services Acquisition	SA-10(04)	TRUSTED GENERATION	Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code,	Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code,		System
System and Services Acquisition	SA-10(05)	MAPPING INTEGRITY FOR VERSION CONTROL	Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the main build data describing the current version of security-relevant hardware, software, and firmware and the on-site main copy of the data for the current	Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the main build data describing the current version of security-relevant hardware, software, and firmware and the on-site main copy of the data for the current		System
System and Services Acquisition	SA-10(06)	TRUSTED DISTRIBUTION	Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates	Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates		System
System and	SA-10(07)	SECURITY AND PRIVACY	Require [Assignment: organization-defined security and privacy representatives] to be included	Require [Assignment: organization-defined security and privacy representatives] to be included		System
System and Services Acquisition	SA-11(02)	Threat Modeling and Vulnerability Analysis	Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that: (a)Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels]; (b)Employs the following tools and methods: [Assignment: organization-defined tools and methods]; (c)Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; and (d)Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].	~~The organization requires~~Require the developer of the ~~information~~ system, system component, or ~~information~~ system service to perform threat modeling and vulnerability analyses during development and the subsequent testing/ and evaluation of the ~~as-built~~ system, component, or service. that: ¶(a)Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];¶(b)Employs the following tools and methods: [Assignment: organization-defined tools and methods];¶(c)Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; and¶(d)Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].		System
System and Services Acquisition	SA-11(03)	INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE	(a) Require an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation; and (b) Verify that the independent agent is provided with sufficient information to complete the	(a) Require an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation; and¶(b) Verify that the independent agent is provided with sufficient information to complete the verification process or		System
System and Services Acquisition	SA-11(04)	MANUAL CODE REVIEWS	Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or techniques].	Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or techniques].		System
System and	SA-11(06)	ATTACK SURFACE	Require the developer of the system, system component, or system service to perform attack	Require the developer of the system, system component, or system service to perform attack		System
System and Services Acquisition	SA-11(07)	VERIFY SCOPE OF TESTING AND EVALUATION	Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigor: [Assignment: organization-defined breadth and depth of testing and	Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigor: [Assignment: organization-defined breadth and depth of testing and		System
System and	SA-11(09)	INTERACTIVE	Require the developer of the system, system component, or system service to employ interactive	Require the developer of the system, system component, or system service to employ interactive		System
System and Services Acquisition	SA-15(01)	QUALITY METRICS	Require the developer of the system, system component, or system service to: (a) Define quality metrics at the beginning of the development process; and (b) Provide evidence of meeting the quality metrics [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review	Require the developer of the system, system component, or system service to:¶(a) Define quality metrics at the beginning of the development process; and¶(b) Provide evidence of meeting the quality metrics [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review milestones]; upon delivery].		System
System and	SA-15(02)	SECURITY AND PRIVACY	Require the developer of the system, system component, or system service to select and employ	Require the developer of the system, system component, or system service to select and employ		System
System and	SA-15(05)	ATTACK SURFACE	Require the developer of the system, system component, or system service to reduce attack	Require the developer of the system, system component, or system service to reduce attack		System
System and	SA-15(06)	CONTINUOUS	Require the developer of the system, system component, or system service to implement an	Require the developer of the system, system component, or system service to implement an		System
System and Services Acquisition	SA-15(07)	AUTOMATED VULNERABILITY ANALYSIS	Require the developer of the system, system component, or system service [Assignment: organization-defined frequency] to: (a) Perform an automated vulnerability analysis using [Assignment: organization-defined tools]; (b) Determine the exploitation potential for discovered vulnerabilities; (c) Determine potential risk mitigations for delivered vulnerabilities; and (d) Deliver the outputs of the tools and results of the analysis to [Assignment: organization-	Require the developer of the system, system component, or system service [Assignment: organization-defined frequency] to:¶(a) Perform an automated vulnerability analysis using [Assignment: organization-defined tools];¶(b) Determine the exploitation potential for discovered vulnerabilities;¶(c) Determine potential risk mitigations for delivered vulnerabilities; and¶(d) Deliver the outputs of the tools and results of the analysis to [Assignment: organization-defined personnel or roles].		System
System and Services Acquisition	SA-15(08)	REUSE OF THREAT AND VULNERABILITY	Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the	Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the		System
System and	SA-15(10)	INCIDENT RESPONSE	Require the developer of the system, system component, or system service to provide, implement,	Require the developer of the system, system component, or system service to provide, implement,		System
System and Services Acquisition	SA-15(11)	ARCHIVE SYSTEM OR COMPONENT	Require the developer of the system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security	Require the developer of the system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security		System
System and	SA-15(12)	MINIMIZE PERSONALLY	Require the developer of the system or system component to minimize the use of personally	Require the developer of the system or system component to minimize the use of personally		System
System and Services Acquisition	SA-16	Developer-Provided Training	Require the developer of the system, system component, or system service to provide training (or training materials) on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms.	~~The organization requires~~Require the developer of the ~~information~~ system, system component, or ~~information~~ system service to provide ~~appropriate~~ training (or training materials)~~, for affected personnel,~~ on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms.		System
System and Services Acquisition	SA-17(01)	FORMAL POLICY MODEL	Require the developer of the system, system component, or system service to: (a) Produce, as an integral part of the development process, a formal policy model describing the [Assignment: organization-defined elements of organizational security and privacy policy] to be enforced; and (b) Prove that the formal policy model is internally consistent and sufficient to enforce the defined	Require the developer of the system, system component, or system service to:¶(a) Produce, as an integral part of the development process, a formal policy model describing the [Assignment: organization-defined elements of organizational security and privacy policy] to be enforced; and¶(b) Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security and privacy policy when implemented.		System
System and Services Acquisition	SA-17(02)	SECURITY-RELEVANT COMPONENTS	Require the developer of the system, system component, or system service to: (a) Define security-relevant hardware, software, and firmware; and (b) Provide a rationale that the definition for security-relevant hardware, software, and firmware is	Require the developer of the system, system component, or system service to:¶(a) Define security-relevant hardware, software, and firmware; and¶(b) Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.		System
System and Services Acquisition	SA-17(03)	FORMAL CORRESPONDENCE	Require the developer of the system, system component, or system service to: (a) Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects; (b) Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model; (c) Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; (d) Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and (e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.	Require the developer of the system, system component, or system service to:¶(a) Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;¶(b) Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model;¶(c) Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;¶(d) Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and¶(e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.		System
System and Services Acquisition	SA-17(04)	INFORMAL CORRESPONDENCE	Require the developer of the system, system component, or system service to: (a) Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects; (b) Show via [Selection: informal demonstration, convincing argument with formal methods as feasible] that the descriptive top-level specification is consistent with the formal policy model; (c) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; (d) Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and (e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.	Require the developer of the system, system component, or system service to:¶(a) Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;¶(b) Show via [Selection: informal demonstration, convincing argument with formal methods as feasible] that the descriptive top-level specification is consistent with the formal policy model;¶(c) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;¶(d) Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and¶(e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.		System
System and Services Acquisition	SA-17(05)	CONCEPTUALLY SIMPLE DESIGN	Require the developer of the system, system component, or system service to: (a) Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and (b) Internally structure the security-relevant hardware, software, and firmware with specific	Require the developer of the system, system component, or system service to:¶(a) Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and¶(b) Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.		System
System and	SA-17(06)	STRUCTURE FOR	Require the developer of the system, system component, or system service to structure security-	Require the developer of the system, system component, or system service to structure security-		System
System and	SA-17(07)	STRUCTURE FOR LEAST	Require the developer of the system, system component, or system service to structure security-	Require the developer of the system, system component, or system service to structure security-		System
System and Services Acquisition	SA-17(08)	ORCHESTRATION	Design [Assignment: organization-defined critical systems or system components] with coordinated behavior to implement the following capabilities: [Assignment: organization-defined	Design [Assignment: organization-defined critical systems or system components] with coordinated behavior to implement the following capabilities: [Assignment: organization-defined		System
System and	SA-17(09)	DESIGN DIVERSITY	Use different designs for [Assignment: organization-defined critical systems or system	Use different designs for [Assignment: organization-defined critical systems or system		System
System and Services Acquisition	SA-20	CUSTOMIZED DEVELOPMENT OF	Reimplement or custom develop the following critical system components: [Assignment: organization-defined critical system components].	Reimplement or custom develop the following critical system components: [Assignment: organization-defined critical system components].		System
System and Services Acquisition	SA-23	SPECIALIZATION	Employ [Selection (one or more): design modification, augmentation, reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission essential	Employ [Selection (one or more): design modification, augmentation, reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission essential		System
System and Communications Protection	SC-02(01)	Interfaces for Non-Privileged Users	Prevent the presentation of system management functionality at interfaces to nonprivileged users.	Prevent the presentation of system management functionality at interfaces to nonprivileged users.	Low, Moderate & High: **Std. 1** - Prevent the presentation of system management functionality at interfaces to nonprivileged users.	System
System and Communications	SC-02(02)	Disassociability	Store state information from applications and software separately.	Store state information from applications and software separately.	Low, Moderate & High: **Std. 1** - Store state information from applications and software separately.	System
System and Communications Protection	SC-03(04)	Module Coupling and Cohesiveness	Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.	~~The organization implements~~Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.		System
System and Communications Protection	SC-03(05)	Layered Structures	Implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	~~The organization implements~~Implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.		System
System and Communications Protection	SC-04(02)	Multilevel or Periods Processing	Prevent unauthorized information transfer via shared resources in accordance with CMS procedures when system processing explicitly switches between different information classification levels or security categories.	Prevent unauthorized information transfer via shared resources in accordance with [CMS RMH procedures ???] when system processing explicitly switches between different information classification levels or security categories.	High & Moderate: Std.1 - Prevent unauthorized information transfer via shared resources in accordance when system processing explicitly switches between different information classification levels or	System
System and Communications	SC-06	Resource Availability	Protect the availability of resources by allocating CMS resources by one or more: priority; quota; controls defined in the applicable security and privacy plan.	Protect the availability of resources by allocating CMS resources by one or more: priority; quota; controls defined in the applicable security and privacy plan.		System
System and Communications Protection	SC-07(09)	Restrict Threatening Outgoing Communications Traffic	(a) Detect and deny outgoing communications traffic posing a threat to external systems; and (b) Audit the identity of internal users associated with denied communications	(a) Detect and deny outgoing communications traffic posing a threat to external systems; and¶(b) Audit the identity of internal users associated with denied communications		System
System and Communications Protection	SC-07(13)	Isolation of security tools, mechanisms, and support	Isolate CMS information security tools, mechanisms, and support components from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.	Isolate CMS information security tools, mechanisms, and support components from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.		System
System and Communications Protection	SC-07(15)	Networked Privileged Access	Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.		System
System and Communications Protection	SC-07(16)	Prevent Discovery of System Components	Prevent the discovery of specific system components that represent a managed interface.	Prevent the discovery of specific system components that represent a managed interface.		System
System and Communications Protection	SC-07(19)	Block Communication from Non-organizationally configured hosts	Block inbound and outbound communications traffic between CMS communication clients that are independently configured by end users and external service providers.	Block inbound and outbound communications traffic between CMS communication clients that are independently configured by end users and external service providers.		System
System and Communications Protection	SC-07(20)	Dynamic Isolation and Segregation	Provide the capability to dynamically isolate CMS system components from other system components.	Provide the capability to dynamically isolate CMS system components from other system components.		System
System and Communications	SC-07(23)	Disable Sender Feedback on Protocol Validation Failure	Disable feedback to senders on protocol format validation failure.	Disable feedback to senders on protocol format validation failure.		System
System and Communications	SC-07(28)	Connections to Public Networks	Prohibit the direct connection of CMS systems to public network.	Prohibit the direct connection of CMS systems to public network.	High & Moderate: **Std. 1** - Prohibit the direct connection of CMS systems to public network.	System
System and Communications Protection	SC-07(29)	Separate Subnets to Isolate Functions	Implement physically or logically separate subnetworks to isolate critical system components and functions.	Implement physically or logically separate subnetworks to isolate critical system components and functions.	High & Moderate: **Std. 1** - Implement physically or logically separate subnetworks to isolate critical system components and functions.	System
System and Communications Protection	SC-8(04)	Conceal or Randomize Communications	Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by alternative physical controls defined in applicable system security and privacy plan.	Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by alternative physical controls defined in applicable system security and privacy plan.		System
System and Communications	SC-08(05)	Protected Distribution System	Implement protected distribution system to prevent unauthorized disclosure of information and detect changes to information during transmission	Implement protected distribution system to prevent unauthorized disclosure of information and detect changes to information during transmission		System
System and Communications Protection	SC-11	Trusted Path	a. Provide a physically and/or logically isolated trusted communications path for communications between the user and the trusted components of the system; and b. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: security functions defined in applicable system security and privacy plan.	a. Provide a physically and/or logically isolated trusted communications path for communications between the user and the trusted components of the system; and¶b. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: security functions defined in applicable system security and privacy plan.	High & Moderate: **Std. 1** - a. Provide a physically and/or logically isolated trusted communications path for communications between the user and the trusted components of the system; and b. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: security functions defined in applicable system security and privacy plan.	System
System and Communications Protection	SC-11(01)	Irrefutable Communications Path	(a) Provide a trusted communications path that is irrefutably distinguishable from other communications paths; and (b) Initiate the trusted communications path for communications between the security functions of the system and the user.	(a) Provide a trusted communications path that is irrefutably distinguishable from other communications paths; and¶(b) Initiate the trusted communications path for communications between the security functions of the system and the user.	High & Moderate: **Std. 1** - (a) Provide a trusted communications path that is irrefutably distinguishable from other communications paths; and (b) Initiate the trusted communications path for communications between the security functions of the system and the user.	System
System and Communications	SC-12(02)	Symmetric Keys	Produce, control, and distribute symmetric cryptographic keys using NIST FIPS-validated key management technology and processes.	Produce, control, and distribute symmetric cryptographic keys using NIST FIPS-validated key management technology and processes.		System
System and Communications Protection	SC-12(03)	Asymmetric Keys	Produce, control, and distribute asymmetric cryptographic keys using one or more of the following: NSA-approved key management technology and processes; prepositioned keying material; DoD-approved Medium Assurance PKI certificates; DoD-approved Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with CMS requirements defined in applicable system security	Produce, control, and distribute asymmetric cryptographic keys using DoD-approved Medium Assurance PKI certificates; DoD-approved Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with CMS requirements defined in applicable system security and privacy plan.		System
System and Communications Protection	SC-12(06)	Physical Control of Keys	Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.	Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.		System
System and Communications Protection	SC-15(01)	Physical or Logical Disconnect	Provide physical and logical disconnect of collaborative computing devices in a manner that supports ease of use.	~~If collaborative computing is authorized, the information system provides~~Provide physical and/or logical disconnect of collaborative computing devices in a manner that supports ease of use.		System
System and Communications Protection	SC-15(03)	Disabling and removal in secure work areas	Disable or remove collaborative computing devices and applications from CMS systems or system components in secure work areas.	Disable or remove collaborative computing devices and applications from CMS systems or system components in secure work areas.		System
System and Communications	SC-15(04)	Explicitly Indicate Current Participants	Provide an explicit indication of current participants in online meetings and teleconferences.	Provide an explicit indication of current participants in online meetings and teleconferences.		System
System and Communications Protection	SC-16	Transmission of Security and Privacy Attributes	Associate security and privacy attributes with information exchanged between systems and between system components.	Associate security and privacy attributes with information exchanged between systems and between system components.		System
System and Communications Protection	SC-16(01)	Integrity Verification	Verify the integrity of transmitted security and privacy attributes.	Verify the integrity of transmitted security and privacy attributes.		System

System and Communications Protection	SC-16(02)	Anti-Spoofing Mechanisms	Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process.
System and Communications Protection	SC-16(03)	Cryptographic Binding	Implement cryptographic mechanisms or techniques (defined in applicable system security and privacy plan) to bind security and privacy attributes to transmitted information.
System and Communications Protection	SC-18(01)	Identify Unacceptable Code and Take Corrective Actions	Identify unacceptable mobile code and take corrective actions.
System and Communications Protection	SC-18(02)	Acquisition, Development, and Use	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets CMS mobile code requirements.
System and Communications Protection	SC-18(03)	Prevent Downloading and Execution	Prevent the download and execution of unacceptable mobile code.
System and Communications Protection	SC-18(05)	Allow Execution Only in Confined Environment	Allow execution of permitted mobile code only in confined virtual machine environments.
System and Communications Protection	SC-20(02)	Data Origin and Integrity	Provide data origin and integrity protection artifacts for internal name/address resolution queries
System and Communications Protection	SC-23(01)	Invalidate Session Identifiers at Logout	Invalidate session identifiers upon user logout or other session termination
System and Communications Protection	SC-23(03)	Unique System-Generated Session Identifiers	Generate a unique session identifier for each session with randomness requirements (as defined in the system security and privacy plan) and recognize only session identifiers that are system generated.
System and Communications Protection	SC-23(05)	Allowed Certificate Authorities	Only allow the use of CMS certificate authorities for verification of the establishment of protected sessions.
System and Communications Protection	SC-25	Thin Nodes	Employ minimal functionality and information storage on the following system components: CMS system components.
System and Communications Protection	SC-26	Decoys	Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.
System and Communications Protection	SC-27	Platform-Independent Applications	Include within organizational systems the following platform independent applications: CMS platform-independent applications.
System and Communications Protection	SC-28(02)	Offline Storage	Remove the following information from online storage and store offline in a secure location: CMS information.
System and Communications Protection	SC-28(03)	Cryptographic Keys	Provide protected storage for cryptographic keys using security safeguards defined in HHS Standard for Encryption of Computing Devices and Information or hardware-protected key store.
System and Communications Protection	SC-29	Heterogeneity	Employ a diverse set of information technologies for the following system components in the implementation of the system: CMS system components (as defined in the applicable system security and privacy plan).
System and Communications Protection	SC-29(01)	Virtualization Techniques	Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed according to frequency defined in the applicable system security and privacy plan.
System and Communications Protection	SC-30	Concealment and Misdirection	Employ concealment and misdirection techniques (defined in the applicable system security and privacy plan) for CMS systems at time periods (defined in the applicable system security and privacy plan) to confuse and mislead adversaries.
System and Communications Protection	SC-30(02)	Randomness	Employ CMS-defined techniques (defined in applicable system security and privacy plan) to introduce randomness into organizational operations and assets.
System and Communications Protection	SC-30(03)	Change Processing and Storage Locations	Change the location of processing and/or storage at time frequency defined in the applicable system security and privacy plan; at random time intervals.
System and Communications Protection	SC-30(04)	Misleading Information	Employ realistic, but misleading information in CMS system components about its security state or posture.
System and Communications Protection	SC-30(05)	Concealment of System Components	Employ techniques (defined in applicable system security and privacy plan) to hide or conceal CMS system components.
System and Communications Protection	SC-31	Covert Channel Analysis	a. Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert storage and/or timing channels; and b. Estimate the maximum bandwidth of those channels.
System and Communications Protection	SC-31(01)	Test Covert Channels for Exploitability	Test a subset of the identified covert channels to determine the channels that are exploitable.
System and Communications Protection	SC-31(02)	Maximum Bandwidth	Reduce the maximum bandwidth for identified covert storage and/or timing channels to CMS-defined values (defined in applicable system security and privacy plan).
System and Communications Protection	SC-31(03)	Measure Bandwidth in Operational Environments	Measure the bandwidth of a subset of identified covert channels (defined in applicable system security and privacy plan) in the operational environment of the system.
System and Communications Protection	SC-32	System Partitioning	Partition the system into defined information system components (defined in the applicable system security and privacy plan) residing in separate physical or logical domains or environments based on defined circumstances (defined in the applicable system security and privacy plan) for physical or logical separation of components.
System and Communications Protection	SC-32(01)	Separate Physical Domains for Privileged Functions	Partition privileged functions into separate physical domains.
System and Communications Protection	SC-34	Non-Modifiable Executable Programs	For CMS system components, load and execute: a. The operating environment from hardware-enforced, read-only media; and b. The following applications from hardware-enforced, read-only media: CMS applications (defined in applicable security system and privacy plan).
System and Communications Protection	SC-34(01)	No Writable Storage	Employ CMS system components with no writeable storage that is persistent across component restart or power on/off.
System and Communications Protection	SC-34(02)	Integrity Protection on Read-only Media	Protect the integrity of information prior to storage on read-only media and control the media after such information has been recorded onto the media.
System and Communications Protection	SC-35	External Malicious Code Identification	Include system components that proactively seek to identify network-based malicious code or malicious websites.
System and Communications Protection	SC-36	Distributed Processing and Storage	Distribute the processing and storage components across multiple physical locations and logical domains.
System and Communications Protection	SC-36(01)	Polling Techniques	(a) Employ polling techniques to identify potential faults, errors, or compromises to the CMS distributed processing and storage components and; (b) Take actions (defined in applicable system security and privacy plan) in response to identified faults, errors, or compromises
System and Communications Protection	SC-36(02)	Synchronization	Synchronize duplicate systems or system components.
System and Communications Protection	SC-37	Out-of-band Channels	Employ out-of-band channels for the physical delivery or electronic transmission of CMS information, system components, or devices to CMS-defined individuals or systems (defined in applicable system security and privacy plan).
System and Communications Protection	SC-37(01)	Ensure Delivery and Transmission	Employ controls (defined in applicable system security and privacy plan) to ensure that only defined individuals or systems (defined in applicable system security and privacy plan) receive CMS information, system components, or devices.
System and Communications Protection	SC-38	Operations Security	Employ operations security controls (defined in applicable system security and privacy plan) to protect key organizational information throughout the system development life cycle.
System and Communications Protection	SC-39(01)	Hardware Separation	Implement hardware separation mechanisms to facilitate process isolation.
System and Communications Protection	SC-39(02)	Separation Execution Domain per Thread	Maintain a separate execution domain for each thread in CMS-defined multi-threaded processing (defined in applicable system security and privacy plan).
System and Communications Protection	SC-40	Wireless Link Protection	Protect external and internal wireless links from the following signal parameter attacks: CMS-defined types of signal parameter attacks (defined in applicable system security and privacy plan)
System and Communications Protection	SC-40(01)	Electromagnetic Interference	Implement cryptographic mechanisms that achieve a level of protection against the effects of intentional electromagnetic interference.
System and Communications Protection	SC-40(02)	Reduce Detection Potential	Implement cryptographic mechanisms to reduce the detection potential of wireless links to CMS-defined level of reduction (defined in applicable system security and privacy plan).
System and Communications Protection	SC-40(3)	Imitative or Manipulative Communications Deception	Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.
System and Communications Protection	SC-40(04)	Signal Parameter Identification	Implement cryptographic mechanisms to prevent the identification of wireless transmitters by using the transmitter signal parameters.
System and Communications Protection	SC-41	Port and I/O Device Access	Physically and Logically disable or remove connection ports or input/output devices on the CMS systems or system components.
System and Communications Protection	SC-42	Sensor Capability and Data	a. Prohibit the use of devices possessing environmental sensing capabilities in CMS facilities, areas, or systems; or the remote activation of environmental sensing capabilities on CMS systems or system components with the following exceptions: where remote activation of sensors is allowed; and b. Provide an explicit indication of sensor use to group of users defined in the CMS IS2P2.
System and Communications Protection	SC-42(01)	Reporting to Authorized Individuals or Roles	Verify that the system is configured so that data or information collected by the sensors (defined in applicable system security and privacy plan) is only reported to authorized individuals or roles.
System and Communications Protection	SC-42(02)	Authorized Use	Employ CMS measures (defined in applicable system security and privacy plan) so that data or information collected by sensors is only used for authorized purposes.
System and Communications Protection	SC-42(04)	Notice of Collection	Employ the following measures to facilitate an individual's awareness that personally identifiable information is being collected by sensors: Conventional written notices and sensor configurations that make individuals aware directly or indirectly through other devices that the sensor is collecting information.
System and Communications Protection	SC-42(05)	Collection Minimization	Employ sensors that are configured to minimize the collection of information about individuals that is not needed.
System and Communications Protection	SC-43	Usage Restrictions	a. Establish usage restrictions and implementation guidelines for CMS system components; and b. Authorize, monitor, and control the use of such components within the system
System and Communications Protection	SC-44	Detonation Chambers	Employ a detonation chamber capability within CMS system, system component, or location.
System and Communications Protection	SC-45	System Time Synchronization	Synchronize system clocks within and between systems and system components.
System and Communications Protection	SC-45(01)	Synchronization with Authoritative Time Source	(a) Compare the internal system clocks defined frequency (defined in applicable system security and privacy plan) with an authoritative time source; and (b) Synchronize the internal system clocks to the authoritative time source when the time difference is greater than defined time period (defined in applicable system security and privacy
System and Communications Protection	SC-45(02)	Secondary Authoritative Time Source	(a) Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source; and (b) Synchronize the internal system clocks to the secondary authoritative time source if the
System and Communications Protection	SC-46	Cross Domain Policy Enforcement	Implement a policy enforcement mechanism physically and logically between the physical and/or network interfaces for the connecting security domains.
System and Communications Protection	SC-47	Alternate Communications Paths	Establish alternate communications paths for system operations organizational command and control.
System and Communications Protection	SC-48	Sensor Relocation	Relocate sensors and monitoring capabilities to locations under CMS-defined conditions or circumstances.
System and Communications Protection	SC-48(1)	Dynamic Relocation of Sensors or Monitoring	Dynamically relocate sensors and monitoring capabilities to locations under CMS conditions or circumstances.
System and Communications Protection	SC-49	Hardware-Enforced Separation and Policy Enforcement	Implement hardware-enforced separation and policy enforcement mechanisms between CMS defined security domains.
System and Communications Protection	SC-50	Software-Enforced Separation and Policy	Implement software-enforced separation and policy enforcement mechanisms between CMS defined security domains.
System and Communications Protection	SC-51	Hardware-Based Protection	a. Employ hardware-based, write-protect for CMS system firmware components; and b. Implement specific procedures for authorized individuals, defined in CMS IS2P2, to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to
System and Information Integrity	SI-02(03)	Time to Remediate Flaws and Benchmarks for Corrective Actions	a. Measure the time between flaw identification and flaw remediation; and b. Establish the following benchmarks for taking corrective actions: 1. Corrective actions must be taken within the time periods defined under the SI-2 (Flaw Remediation) Implementation Standards.
System and Information Integrity	SI-02(04)	Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to system components.
System and Information Integrity	S1-02(05)	Automatic Software and Firmware Updates	Install security-relevant software and firmware updates (defined in applicable system security/privacy plan) automatically to system components.
System and Information Integrity	SI-03(04)	Updates only by Privileged Users	Update malicious code protection mechanisms only when directed by a privileged user.
System and Information Integrity	SI-03(06)	Testing and Verification	(a) Test malicious code protection mechanisms CMS Mission/Business/System-defined frequency (defined in applicable system security/privacy plan) by introducing known benign code into the system; and
System and Information Integrity	SI-03(08)	Detect Unauthorized Commands	(a) Detect the following unauthorized operating system commands through the kernel application programming interface on system hardware components (defined in applicable system security/privacy plan): unauthorized operating system commands (defined in applicable system security/privacy plan); and (b) Issue a warning, audit the command execution and/or prevent the execution of the command.
System and Information Integrity	SI-03(10)	Malicious Code Analysis	(a) Employ CMS CCIC approved tools and techniques to analyze the characteristics and behavior of malicious code; and (b) Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.
System and Information Integrity	SI-04(03)	Automated Tool and Mechanism Integration	Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms.
System and Information Integrity	SI-04(07)	Automated Response to Suspicious Events	(a) Notify CMS CCIC of detected suspicious events; and (b) Take the following action upon detection: the least disruptive actions to terminate suspicious
System and Information Integrity	SI-04(09)	Testing of Monitoring Tools and Mechanisms	Test intrusion-monitoring tools and mechanisms according to frequency defined in applicable system security/privacy plan.
System and Information Integrity	SI-04(15)	Wireless to Wireline Communications	Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.
System and Information Integrity	SI-04(17)	Integrated Situational Awareness	Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.
System and Information Integrity	SI-04(19)	Risk for Individuals	Implement additional monitoring (defined in applicable system security/privacy plan) of individuals who have been identified by CMS-defined sources as posing an increased level of risk.
System and Information Integrity	SI-04(21)	Probationary Periods	Implement the additional monitoring of individuals during CMS defined probationary period
System and Information Integrity	SI-04(24)	Indicators of Compromise	Discover, collect, and distribute to applicable personnel or roles (e.g. CMS CCIC personnel, ISSO), indicators of compromise provided by defined sources.
System and Information Integrity	SI-04(25)	Optimize Network Traffic Analysis	Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.
System and Information Integrity	SI-06(02)	Automation Support for	Implement automated mechanisms to support the management of distributed security and privacy
System and Information Integrity	SI-06(03)	Report Verification Results	Report the results of security and privacy function verification to CMS personnel or roles
System and Information Integrity	SI-07(03)	Centrally Managed Integrity	Employ centrally managed integrity verification tools.
System and Information Integrity	SI-07(06)	Cryptographic Protection	Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.
System and Information Integrity	SI-07(08)	Auditing Capability for Significant Events	Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: generate an audit record, alert current user and alert CMS-defined
System and Information Integrity	SI-07(09)	Verify Boot Process	Verify the integrity of the boot process of the system components.
System and Information Integrity	SI-07(10)	Protection of Boot Firmware	Implement the following mechanisms to protect the integrity of boot firmware in system components: CMS-defined mechanisms defined in the applicable system security/privacy plan.
System and Information Integrity	SC-07(12)	Integrity Verification	Require that the integrity of the user-installed software (defined in the applicable system security/privacy plan) be verified prior to execution.
System and Information Integrity	SI-07(16)	Time limit on Process Execution Without Supervision	Prohibit processes from executing without supervision for more than time period defined in applicable system security/privacy plan.
System and Information Integrity	SC-07(17)	Runtime Application Self-Protection	Implement controls (defined in the applicable System Security and Privacy Plan) for application self-protection at runtime.
System and Information Integrity	SI-08(03)	Continuous Learning	Implement spam protection mechanisms with a learning capability to more effectively identify
System and Information Integrity	SI-10(01)	Manual Override Capability	(a) Provide a manual override capability for input validation of the information inputs defined in the base control (SI-10); (b) Restrict the use of the manual override capability to only CMS defined authorized individuals (defined in the applicable system security/privacy plan); and
System and Information Integrity	SI-10(02)	Review and Resolve Errors	Review and resolve input validation errors within time defined in applicable system security/privacy plan.
System and Information Integrity	SI-10(03)	Predictable Behavior	Verify that the system behaves in a predictable and documented manner when invalid inputs are received.
System and Information Integrity	SI-10(04)	Timing Interactions	Account for timing interactions among system components in determining appropriate responses for invalid inputs.
System and Information Integrity	SI-10(05)	Restrict Inputs to Trusted Sources and Approved	Restrict the use of information inputs to trusted sources and/or formats.
System and Information Integrity	SI-10(06)	Injection Prevention	Prevent untrusted data injections.
System and Information Integrity	SI-13	Predictable Failure Prevention	a. Determine mean time to failure (MTTF) for system components in specific environments of operation; and b. Provide substitute system components and a means to exchange active and standby components in accordance with the MTTF substitution criteria.
System and Information Integrity	SI-13(01)	Transferring Component Responsibilities	Take system components out of service by transferring component responsibilities to substitute components no later than CMS-defined fraction or percentage (defined in applicable contingency plan) of mean time to failure.
System and Information Integrity	SI-13(03)	Manual Transfer Between Components	Manually initiate transfers between active and standby system components when the use of the active component reaches a specified percentage (defined in the applicable contingency Plan) of the mean time to failure.
System and Information Integrity	SI-13(04)	Standby Component Installation and Notification	If system component failures are detected: (a) Ensure that the standby components are successfully and transparently installed within time period defined in applicable contingency plan; and
System and Information Integrity	SI-13(05)	Failover Capability	Provide real-time or near real-time failover capability for the system.

System and Information Integrity	SI-14	Non-Persistence	Implement non-persistent system components and services that are initiated in a known state and terminated: upon end of session of use or periodically as defined by the Organizations Mission/Business functions.	Implement non-persistent system components and services that are initiated in a known state and terminated: upon end of session of use or periodically as defined by the Organizations Mission/Business functions.		System	Not Specified	Three (3) Years	Above Baseline	This control mitigates risk from advanced persistent threats (APTs) by significantly reducing the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete attacks. By implementing the concept of non-persistence for selected system components, organizations can provide a known state computing resource for a specific time-period that does not give adversaries sufficient time to exploit vulnerabilities in organizational systems and the environments in which those systems operate. Since the APT is a high-end, sophisticated threat regarding capability, intent, and targeting, organizations assume that over an extended period, a percentage of attacks will be successful. Non-persistent system components and services are activated as required using protected information and terminated periodically or at the end of sessions. Non-persistence increases the workfactor of adversaries in attempting to compromise or breach organizational systems. Non-persistence can be achieved by refreshing system components by periodically re-imaging components or by using a variety of common virtualization techniques. Non-persistent services can be implemented by using virtualization techniques as part of virtual machines or as new instances of processes on physical machines (either persistent or non persistent). The benefit of periodic refreshes of system components and services is that it does not require organizations to first determine whether compromises of components or services have occurred (something that may often be difficult to determine). The refresh of selected system components and services occurs with sufficient frequency to prevent the spread or intended impact of attacks, but not with such frequency that it makes the system unstable. Refreshes of critical components and services may be done periodically to hinder the ability of adversaries to exploit optimum windows of vulnerabilities.		SC-30, SC-34, SI-21	None.					
System and	SI-14(01)	Refresh From Trusted	Obtain software and data employed during system component and service refreshes from trusted	Obtain software and data employed during system component and service refreshes from trusted		System	Not Specified	Three (3) Years	Above Baseline	Trusted sources include software and data from write-once, read-only media or from		None.	None.					
System and Information Integrity	SI-14(02)	Non-Persistent Information	(a) Refresh information annually; generate information on demand; and (b) Delete information when no longer needed.	(a) Refresh information annually; generate information on demand; and¶(b) Delete information when no longer needed.		System	Not Specified	Three (3) Years	Above Baseline	Retaining information longer than it is needed makes the information a potential target for advanced adversaries searching for high value assets to compromise through unauthorized disclosure, unauthorized modification, or exfiltration. For system-related information, unnecessary retention provides advanced adversaries information that can		None.	None.					
System and Information Integrity	SI-14(03)	Non-Persistent Connectivity	Establish connections to the system on demand and terminate connections after completion of a request or a period of non-use.	Establish connections to the system on demand and terminate connections after completion of a request or a period of non-use.		System	Not Specified	Three (3) Years	Above Baseline	Persistent connections to systems can provide advanced adversaries with paths to move laterally through systems, and potentially position themselves closer to high value assets. Limiting the availability of such connections impedes the adversary's ability to move freely		SC-10	None.					
System and Information Integrity	SC-15	Information Output Filtering	Validate information output from software programs and/or applications to ensure that the information is consistent with the expected content.	Validate information output from software programs and/or applications to ensure that the information is consistent with the expected content.		System	Not Specified	Three (3) Years	Above Baseline	Certain types of attacks, including SQL injections, produce output results that are unexpected or inconsistent with the output results that would be expected from software programs or applications. Information output filtering focuses on detecting extraneous content, preventing such extraneous content from being displayed, and then alerting		SI-3, SI-4, SI-11.	None.					
System and Information Integrity	SI-17	Fail-Safe Procedures	Implement the indicated fail-safe procedures when the indicated failures occur: fail-safe procedures identified in SC-07(18).	Implement the indicated fail-safe procedures when the indicated failures occur: fail-safe procedures identified in SC-07(18).		System	Not Specified	Three (3) Years	Above Baseline	Failure conditions include the loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include alerting operator personnel and providing specific instructions on subsequent steps to take. Subsequent steps may include doing nothing, reestablishing system settings,		CP-12, CP-13, SC-24, SI-13.	None.					
System and Information Integrity	SI-18(01)	Automation Support	Correct or delete personally identifiable information that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified using automated mechanisms defined in the applicable System Security and Privacy Plan.	Correct or delete personally identifiable information that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified using automated mechanisms defined in the applicable System Security and Privacy Plan.		System	Not Specified	Three (3) Years	Above Baseline	The use of automated mechanisms to improve data quality may inadvertently create privacy risks. Automated tools may connect to external or otherwise unrelated systems, and the matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan. As data is obtained and used across the information life cycle, it is important to confirm the accuracy and relevance of personally identifiable information. Automated mechanisms can augment existing data quality processes and procedures and enable an organization to better identify and manage personally identifiable information in large-scale systems. For example, automated tools can greatly improve efforts to consistently normalize data or identify malformed data. Automated tools can also be used to improve auditing of data and detect errors that may incorrectly alter personally identifiable information or incorrectly associate such information with the wrong individual. Automated capabilities backstop processes and procedures at-scale and enable more fine-grained detection and correction		PM-18, PM-22, RA-8	See Control SI-18.					
System and Information Integrity	SI-18(02)	Data Tags	Employ data tags to automate the correction or deletion of personally identifiable information across the information life cycle within organizational systems.	Employ data tags to automate the correction or deletion of personally identifiable information across the information life cycle within organizational systems.		System	Not Specified	Three (3) Years	Above Baseline	Data tagging personally identifiable information includes tags noting processing permissions, authority to process, de-identification, impact level, information life cycle stage, and retention or last updated dates. Employing data tags for personally identifiable information can support the use of automation tools to correct or delete relevant personally		AC-3, AC-16, SC-16	See Control SI-18.					
System and Information Integrity	SI-18(03)	Collection	Collect personally identifiable information directly from the individual.	Collect personally identifiable information directly from the individual.		System	Not Specified	Three (3) Years	Above Baseline	Individuals, or their designated representatives, can be a source of correct personally identifiable information about themselves. Organizations consider contextual factors that may incentivize individuals to provide correct data versus providing false data. Additional steps may be necessary to validate collected information based on the nature and context of the personally identifiable information, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of personally identifiable information used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive personally		None.	See Control SI-18.					
System and Information Integrity	SI-18(05)	Notice of Collection or Deletion	Notify recipients of personally identifiable information and individuals that the personally identifiable information has been corrected or deleted.	Notify recipients of personally identifiable information and individuals that the personally identifiable information has been corrected or deleted.		System	Not Specified	Three (3) Years	Above Baseline	When personally identifiable information is corrected or deleted, organizations take steps to ensure that all authorized recipients of such information, and the individual with which the information is associated or their designated representative, are informed of the corrected		None.	See Control SI-18.					
System and Information Integrity	SI-19(01)	Collection	De-identify the dataset upon collection by not collecting personally identifiable information.	De-identify the dataset upon collection by not collecting personally identifiable information.		System	Not Specified	Three (3) Years	Above Baseline	If a data source contains personally identifiable information but the information will not be used, the dataset can be de-identified upon creation by not collecting the data elements containing the personally identifiable information. For example, if an organization does not intend to use the social security number of an applicant, then application forms do not ask		None.	See Control SI-19.					
System and Information Integrity	SI-19(02)	Archiving	Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived.	Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived.		System	Not Specified	Three (3) Years	Above Baseline	Datasets can be archived for many reasons. The envisioned purposes for the archived dataset are specified and if personally identifiable information elements are not required, the elements are not archived. For example, social security numbers may have been collected for record linkage, but the archived dataset may include the required elements from the linked records. In this case, it is not necessary to archive the social security		None.	See Control SI-19.					
System and Information Integrity	SI-19(03)	Release	Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.	Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.		System	Not Specified	Three (3) Years	Above Baseline	Prior to releasing a dataset, a data custodian considers the intended uses of the dataset and determines if it is necessary to release personally identifiable information. If the personally identifiable information is not necessary, the information can be removed using		None.	See Control SI-19.					
System and Information Integrity	SI-19(04)	Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers	Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.	Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.		System	Not Specified	Three (3) Years	Above Baseline	There are many possible processes for removing direct identifiers from a dataset. Columns in a dataset that contain a direct identifier can be removed. In masking, the direct identifier is transformed into a repeating character, for example, XXXXXX or 999999. Identifiers can be encrypted or hashed, so that the linked records remain linked. In the case of encryption or hashing, algorithms are employed that require the use of a key, including the Advanced Encryption Standard or a Hash-based Message Authentication Code. Implementations may use the same key for all identifiers or use a different key for each identifier. Using a different key for each identifier provides for a higher degree of security and privacy. Identifiers can alternatively be replaced with a keyword, including transforming "George Washington" to "PATIENT," or replaced with a surrogate value, for example,		SC-12, SC-13	See Control SI-19.					
System and Information Integrity	SI-19(05)	De-identification | Statistical Disclosure Control	Manipulate numerical data, contingency tables, and statistical findings so that no person or organization is identifiable in the results of the analysis.	Manipulate numerical data, contingency tables, and statistical findings so that no person or organization is identifiable in the results of the analysis.		System	Not Specified	Three (3) Years	Above Baseline	Many types of statistical analyses can result in the disclosure of information about individuals even if only summary information is provided. For example, if a school publishes a monthly table with the number of minority students, and in January the school reports that it has 10-19 such students, but in March it reports that it has 20-29 students, then it can be		None.	See Control SI-19.					
System and Information Integrity	SI-19(06)	Differential Privacy	Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported.	Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported.		System	Not Specified	Three (3) Years	Above Baseline	The mathematical definition for differential privacy holds that the result of a dataset analysis should be approximately the same before and after the addition or removal of a single data record (which is assumed to be the data from a single individual). In its most basic form, differential privacy applies only to online query systems. However, it can also be used to produce machine-learning statistical classifiers and synthetic data. Differential privacy comes at the cost of decreased accuracy of results, forcing organizations to quantify the trade-off between privacy protection and the overall accuracy, usefulness, and utility of the de-identified dataset. Non-deterministic noise can include adding small random values to		SC-12, SC-13	See Control SI-19.					
System and Information Integrity	SI-19(07)	Validated Algorithms Software	Perform de-identification using validated algorithms and software that is validated to implement the algorithms.	Perform de-identification using validated algorithms and software that is validated to implement the algorithms.		System	Not Specified	Three (3) Years	Above Baseline	Algorithms that appear to remove personally identifiable information from a dataset may in fact leave information that is personally identifiable or data that are re-identifiable. Software that is claimed to implement a validated algorithm may contain bugs or may implement a different algorithm. Software may de-identify one type of data, for example, integers, but not another type of data, for example, floating point numbers. For these reasons, de-		None.	See Control SI-19.					
System and Information Integrity	SI-19(08)	Motivated Intruder	Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.	Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.		System	Not Specified	Three (3) Years	Above Baseline	A motivated intruder test is a test in which a person or group takes a data release and specified resources and attempts to re-identify one or more individuals in the de-identified dataset. Such tests specify the amount of inside knowledge, computational resources, financial resources, data, and skills that intruders have at their disposal to conduct the tests. A motivated intruder test can determine if de-identification is insufficient. It can also be a useful diagnostic tool to assess if de-identification is likely to be sufficient. However,		None.	[OMB A-130, Appendix II];NIST [SP 800-188].					
System and Information Integrity	SI-20	Tainting	Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: CMS systems or system components.	Embed data or capabilities in the following systems or system components to¶determine if organizational data has been exfiltrated or improperly removed from the¶organization: CMS systems or system components.		System	Not Specified	Three (3) Years	Above Baseline	Many cyber-attacks target organizational information (or sensitive information the organization holds on behalf of other entities (e.g., personally identifiable information) and exfiltrate that data. In addition, insider attacks and erroneous user procedures can remove information from the system in violation of the organizational policies. Tainting approaches can range from passive to active. A passive tainting approach can be as simple as adding false email names and addresses to an internal database. If the organization receives email at one of the false email addresses, it knows that the database has been compromised. Moreover, the organization knows that the email was sent by an unauthorized entity so any packets it includes potentially contain malicious code and that the unauthorized entity potentially has obtained a copy of the database. A less passive tainting approach can include embedding false data or steganographic data in files to enable the data to be found via open source analysis. And finally, an active tainting approach can include embedding software in the data that is able to "call home" alerting the organization		AU-13	[OMB A-130, Appendix II]; [SP 800-160 v2].					
System and Information Integrity	SI-21	Information Refresh	Refresh critical or sensitive information at frequencies (defined in applicable System Security and Privacy Plan) or generate the information on demand and delete the information when no longer needed.	Refresh critical or sensitive information at frequencies (defined in applicable System Security and Privacy Plan) or generate the information on demand and delete the information when no longer needed.		System	Not Specified	Three (3) Years	Above Baseline	Retaining critical or sensitive information (e.g., classified information or controlled unclassified information) for longer than it is needed makes it an increasing valuable and enticing target for adversaries. Keeping such information available for the minimum period of time needed for mission accomplishment reduces the opportunity for adversaries to		SI-14	[OMB A-130]; NIST [SP 800-160 v2].					
System and Information Integrity	SI-22	Information Diversity	a. Identify the CMS defined alternative sources of information for essential functions and services: e.g. non-digitally obtained data and multiple data sources; and b. Use an alternative information source for the execution of essential functions or services on systems or system components when the primary source of information is corrupted or unavailable.	a. Identify the CMS defined alternative sources of information for essential functions and services: e.g. non-digitally obtained data and multiple data sources; and¶b. Use an alternative information source for the execution of essential functions or services on systems or system components when the primary source of information is corrupted or unavailable.	**Std. 1** - Ensure information provided from different sources or transformed in different ways are in accordance with NIST SP 800-160, as amended.	System	Not Specified	Three (3) Years	Above Baseline	Actions taken by a system service or a function are often driven by the information it receives. Corruption, fabrication, modification, or deletion of that information could impact the ability of the service function to properly carry out its intended actions. By having multiple sources of input, the service or function can continue operation if one source is corrupted or no longer available. It is possible that the alternative sources of information may be less precise or less accurate than the primary source of information. But having such sub-optimal information sources may still provide a sufficient level of quality that the		None.	[SP 800-160 v2].					
System and Information Integrity	SI-23	Information Fragmentation	Based on CMS defined circumstances: a. Fragment the following information: e.g. sensitive and valuable information; and b. Distribute the fragmented information across the systems or system components.	Based on CMS defined circumstances:¶a. Fragment the following information: e.g. sensitive and valuable information; and¶b. Distribute the fragmented information across the systems or system components.	**Std. 1** - Implement fragmentation and partitioning for distributed databases in accordance with NIST SP 800-160, as amended.	System	Not Specified	Three (3) Years	Above Baseline	One major objective of the advanced persistent threat is to exfiltrate sensitive and valuable information. Once exfiltrated, there is generally no way for the organization to recover the lost information. Therefore, organizations may consider taking the information and dividing it into disparate elements and then distributing those elements across multiple systems or system components and locations. Such actions will increase the adversary's work factor to capture and exfiltrate the desired information and in so doing, increase the probability of detection. The fragmentation of information also impacts the organization's ability to access the information in a timely manner. The extent of the fragmentation would likely be dictated by the sensitivity (and value) of the information, threat intelligence information received, and if data tainting is used (i.e., data tainting derived information about exfiltration		None.	[SP 800-160 v2].					
Supply Chain Risk Management	SR-03(01)	Diverse Supply Base	Employ a diverse set of sources for the following system components and services: (a) OIT- and CISO-defined system components and services (defined through CIO-level policies); and (b) Business/System-defined system components and services (defined in applicable security/privacy plans).	Employ a diverse set of sources for the following system components and services:¶(a) OIT- and CISO-defined system components and services (defined through CIO-level policies); and¶(b) Business/System-defined system components and services (defined in applicable security/privacy plans).	**High, Moderate & Low:** **Std. 1** - Employ a diverse set of sources for the following system components and services: (a) OIT- and CISO-defined system components and services (defined through CIO-level policies); and (b) Business/System-defined system components and services (defined in applicable security/privacy plans).	OCISO System	Not Specified	Three (3) Years	Above Baseline	Diversifying the supply of systems, system components, and services can reduce the probability that adversaries will successfully identify and target the supply chain and can reduce the impact of a supply chain event or compromise. Identifying multiple suppliers for replacement components can reduce the probability that the replacement component will become unavailable. **Employing a diverse set of developers or logistics service providers can reduce the impact of a natural disaster or other supply chain event. Organizations consider designing the system to include diverse materials and**	P2	None;	See SR-3;					
Supply Chain Risk Management	SR-03(02)	Limitation of Harm	Employ the following supply chain controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: (a) OIT- and CISO-defined supply chain controls (defined through CIO-level policies); and (b) Business/System-defined supply chain controls (defined in applicable security/privacy plans).	Employ the following supply chain controls to limit harm from potential adversaries identifying and targeting the organizational supply chain:¶(a) OIT- and CISO-defined supply chain controls (defined through CIO-level policies); and¶(b) Business/System-defined supply chain controls (defined in applicable security/privacy plans).	High, Moderate & Low: **Std. 1** - The organization must comply with guidelines detailed in the HHS Policy for Cyber Supply Chain Risk Management.	OCISO System	Not Specified	Three (3) Years	Above Baseline	Controls that can be implemented to reduce the probability of adversaries successfully identifying and targeting the supply chain include avoiding the purchase of custom or non-standardized configurations, employing approved vendor lists with standing reputations in industry, following pre-agreed maintenance schedules and update and patch delivery mechanisms, maintaining a contingency plan in case of a supply chain event, using procurement carve-outs that provide exclusions to commitments or obligations, using diverse delivery routes, and minimizing the time between purchase decisions and delivery.	P2	None;	See SR-3;					
Supply Chain Risk Management	SR-03(03)	Sub-tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.	High, Moderate & Low: **Std. 1** - The organization must adhere to the HHS Policy for Information Technology Procurements - Security And Privacy Language.	System	Not Specified	Three (3) Years	Above Baseline	To manage supply chain risk effectively and holistically, it is important that organizations ensure that supply chain risk management controls are included at all tiers in the supply chain. This includes ensuring that Tier 1 (prime) contractors have implemented processes to facilitate the "flow down" of supply chain risk management controls to sub-tier		SR-5, SR-8;	See SR-3;					
Supply Chain Risk Management	SR-04	Provenance	Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: (a) OIT and CISO-defined systems, system components, and associated data (defined through CIO-level policies); and (b) Business/System-defined systems, system components, and associated data (defined in applicable security/privacy plans).	Document, monitor, and maintain valid provenance of the following systems, system components, and associated data:¶(a) OIT and CISO-defined systems, system components, and associated data (defined through CIO-level policies); and¶(b) Business/System-defined systems, system components, and associated data (defined in applicable security/privacy plans).	**High, Moderate & Low:** **Std. 1** - Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: (a) OIT and CISO-defined systems, system components, and associated data (defined through CIO-level policies); and (b) Business/System-defined systems, system components, and associated data (defined in applicable security/privacy plans).	OCISO System	Not Specified	Three (3) Years	Above Baseline	Every system and system component has a point of origin and may be changed throughout its existence. **Provenance is the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data.** Organizations consider developing procedures (see SR-1) for allocating responsibilities for the creation, maintenance, and monitoring of provenance for systems and system components; transferring provenance documentation and responsibility between organizations; and preventing and monitoring for unauthorized changes to the provenance records. Organizations have methods to document, monitor, and maintain valid provenance baselines for systems, system components, and related data. These actions help track, assess, and document any changes to the provenance, including changes in supply chain elements or configuration, and help ensure non-repudiation of provenance information and the provenance change records. Provenance considerations are addressed throughout the system development life cycle and incorporated into contracts and other arrangements, as	P1	CM-8, MA-2, MA-6, RA-9, SA-3, SA-8, SI-4;	NIST SP: 800-161, 800-161-1; NISTIR: 7622; 8112; 8272 FASC18, 41 CFR 201, EO 13873, ISO 27036, ISO 20243;					
Supply Chain Risk Management	SR-04(01)	Identity	Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components: (a) OIT and CISO-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components (defined through CIO-level policies); and (b) Business/System-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components (defined in applicable security/privacy plans).	Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components:¶(a) OIT and CISO-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components (defined through CIO-level policies); and¶(b) Business/System-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components (defined in applicable security/privacy plans).	**High, Moderate & Low:** **Std. 1** - Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components: (a) OIT and CISO-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components (defined through CIO-level policies); and (b) Business/System-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components (defined in applicable security/privacy plans).	OCISO System	Not Specified	Three (3) Years	Above Baseline	Knowing who and what is in the supply chains of organizations is critical to gaining visibility into supply chain activities. Visibility into supply chain activities is also important for monitoring and identifying high-risk events and activities. Without reasonable visibility into supply chains elements, processes, and personnel, it is very difficult for organizations to understand and manage risk and reduce their susceptibility to adverse events. Supply chain elements include organizations, entities, or tools used for the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems and system components. Supply chain processes include development processes for hardware, software, and firmware; shipping and handling procedures; configuration management tools, techniques, and measures to maintain provenance; personnel and physical security programs; or other programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain personnel are individuals with specific roles and responsibilities related to the secure the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of a system or system component. Identification methods are sufficient to support an investigation in case of a supply chain change (e.g. if a supply company is purchased), compromise, or event.	P2	IA-2; IA-8, PE-16;	See SR-4;					
Supply Chain Risk Management	SR-04(04)	Supply Chain Integrity - Pedigree	Employ OIT- and CISO-defined controls (defined in applicable security/privacy plans) and conduct OIT- and CISO-defined analysis (defined in applicable security/privacy plans) to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission essential technologies, products, and services.	Employ OIT- and CISO-defined controls (defined in applicable security/privacy plans) and conduct OIT- and CISO-defined analysis (defined in applicable security/privacy plans) to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission essential technologies, products, and services.	**High, Moderate & Low:** **Std. 1** - Employ OIT- and CISO-defined controls (defined in applicable security/privacy plans) and conduct OIT- and CISO-defined analysis (defined in applicable security/privacy plans) to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission essential technologies, products, and services.	System	Not Specified	Three (3) Years	Above Baseline	Authoritative information regarding the internal composition of system components and the provenance of technology, products, and services provides a strong basis for trust. The validation of the internal composition and provenance of technologies, products, and services is referred to as the pedigree. For microelectronics, this includes material composition of components. For software this includes the composition of opensource and proprietary code, including the version of the component at a given point in time. Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid. The validation of the internal composition and provenance can be achieved by various evidentiary artifacts or records that manufacturers and suppliers produce during the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of technology, products, and services. Evidentiary artifacts include, but are not limited to, software identification (SWID) tags, software component inventory, the manufacturers' declarations of platform attributes (e.g., serial numbers, hardware component inventory), and measurements (e.g., firmware hashes) that are tightly		RA-3	See SR-4;					
Supply Chain Risk Management	SR-05(01)	Adequate Supply	Employ the following controls to ensure an adequate supply of: (a) OIT- and CISO-defined critical system components and component controls (defined through CIO-level policies); and (b) Business/System-defined critical system components and component controls (defined in applicable security/privacy plans).	Employ the following controls to ensure an adequate supply of:¶(a) OIT- and CISO-defined critical system components and component controls (defined through CIO-level policies); and¶(b) Business/System-defined critical system components and component controls (defined in applicable security/privacy plans).	**High & Moderate:** **Std. 1** - Employ the following controls to ensure an adequate supply of: (a) OIT- and CISO-defined critical system components and component controls (defined through CIO-level policies); and (b) Business/System-defined critical system components and component controls (defined in applicable security/privacy plans).	OCISO System	Not Specified	Three (3) Years	Above Baseline	Adversaries can attempt to impede organizational operations by disrupting the supply of critical system components or corrupting supplier operations. Organizations may track systems and component mean time to failure to mitigate the loss of temporary or permanent system function. Controls to ensure that adequate supplies of critical system components include the use of multiple suppliers throughout the supply chain for the identified critical components, stockpiling spare components to ensure operation during mission critical times, and the identification of functionally identical or similar components that may be	P2	RA-9;	See SR-5;					
Supply Chain Risk Management	SR-06(01)	Testing and Analysis	Employ Business/System-sponsored analysis, independent third-party analysis, Business/System-sponsored testing, CMS CCIC penetration testing, and/or independent third-party testing of the following supply chain elements, processes, and actors associated with the system, system component, or system service: (a) OIT- and CISO-defined supply chain elements, processes, and actors (defined through CIO-level policies); and (b) Business/System-defined supply chain elements, processes, and actors(defined in applicable security/privacy plans).	Employ Business/System-sponsored analysis, independent third-party analysis, Business/System-sponsored testing, CMS CCIC penetration testing, and/or independent third-party testing of the following supply chain elements, processes, and actors associated with the system, system component, or system service:¶(a) OIT- and CISO-defined supply chain elements, processes, and actors (defined through CIO-level policies); and¶(b) Business/System-defined supply chain elements, processes, and actors(defined in applicable security/privacy plans).	**High & Moderate:** **Std. 1** - Employ Business/System-sponsored analysis, independent third-party analysis, Business/System-sponsored testing, CMS CCIC penetration testing, and/or independent third-party testing of the following supply chain elements, processes, and actors associated with the system, system component, or system service: (a) OIT- and CISO-defined supply chain elements, processes, and actors (defined through CIO-level policies); and (b) Business/System-defined supply chain elements, processes, and actors(defined in applicable security/privacy plans).	OCISO System	Not Specified	Three (3) Years	Above Baseline	Relationships between entities and procedures within the supply chain, including development and delivery, are considered. Supply chain elements include organizations, entities, or tools that are used for the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems, system components, or system services. Supply chain processes include supply chain risk management programs; SCRM strategies and implementation plans; personnel and physical security programs; hardware, software, and firmware development processes; configuration management tools, techniques, and measures to maintain provenance; shipping and handling procedures; and programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain actors are individuals with specific roles and responsibilities in the supply chain. The evidence generated and collected during analyses and testing of supply chain elements, processes, and actors is documented and used to inform organizational risk management activities	P2	CA-8, SI-4;	See SR-6;					
Supply Chain Risk Management	SR-07	Supply Chain Operations Security	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: (a) OIT- and CISO-defined OPSEC controls (defined through CIO-level policies); and (b) Business/System-defined OPSEC controls(defined in applicable security/privacy plans).	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service:¶(a) OIT- and CISO-defined OPSEC controls (defined through CIO-level policies); and¶(b) Business/System-defined OPSEC controls(defined in applicable security/privacy plans).	**High & Moderate:** **Std. 1** - Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: (a) OIT- and CISO-defined OPSEC controls (defined through CIO-level policies); and (b) Business/System-defined OPSEC controls(defined in applicable security/privacy plans).	OCISO System	Not Specified	Three (3) Years	Above Baseline	Supply chain OPSEC expands the scope of OPSEC to include suppliers and potential suppliers. OPSEC is a process that includes identifying critical information, analyzing friendly actions related to operations and other activities to identify actions that can be observed by potential adversaries, determining indicators that potential adversaries might obtain that could be interpreted or pieced together to derive information in sufficient time to cause harm to organizations, implementing safeguards or countermeasures to eliminate or reduce exploitable vulnerabilities and risk to an acceptable level, and considering how aggregated information may expose users or specific uses of the supply chain. Supply chain information includes user identities; uses for systems, system components, and system services; supplier identities; security and privacy requirements; system and component configurations; supplier processes; design specifications; and testing and evaluation results. Supply chain OPSEC may require organizations to withhold mission or business information from suppliers and may include the use of intermediaries to hide the	P2	SC-38;	NIST SP: 800-30, 800-161; NISTIR: 7622; EO 13873, ISO 27036					
Supply Chain Risk Management	SR-11(03)	Anti-counterfeit Scanning	Scan for counterfeit system components no less often than every 365 days.	Scan for counterfeit system components no less often than every 365 days.	**High, Moderate & Low:** **Std. 1** - Scan for counterfeit system components no less often than every 365 days.	System	Not Specified	Three (3) Years	Above Baseline	The type of component determines the type of scanning to be conducted (e.g., web application scanning if the component is a web application). The scanning method employed by CMS Businesses/Systems to detect the counterfeit component use within the supply chain will be dependent on the tool and industry standard associated with the component being evaluated. There are multiple standards associated with each type of component addressing inspection, test, and authentication (IT&A). Regretfully, each standard deals with inspection methods, counterfeit detection policies, advanced testing methods, and ensuring authenticity differently. This means that not all IT&A tests will be the same – resulting in variation in terms of detail and rigor. The five best known sources for SCRM standards include the *Independent Distributors of Electronics Association* (IDEA), *the Joint Electron Device Engineering Council* (JEDEC), Institute of Printed Circuits (IPC), the *Society of Automotive Engineers* (SAE) International, and the *Defense Logistics Agency* (DLA). Each source defines its own criteria (e.g., sampling, non-destructive and destructive tests) used in the assessment.	P2	RA-5;	NISTIR: 7622; ISO 20243.					

Centers for Medicare & Medicaid Services (CMS)

Business Partners

Systems Security Manual

CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

(Rev.11570, Issued:08-19-22)

CMS/ Business Partners
Systems Security Manual

Record of Changes

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Revision	Major Changes	Date
12	Main Document and all Appendices (1) Updated Internet hyperlinks throughout document (2) Changed “EISG” (Enterprise Information Security Group) to “ISPG” (Information Security and Privacy Group” throughout document (3) Correct typographical errors	08/2013
13	Main Document and all Appendices (1) Deleted Section 3.6.1/Computer Security Incident Response due to duplication (2) Added Section 3.12/End Of Life Technology Components (3) Added Section 3.13/Cloud Computing (4) Added Attachment 1/MAC ARS	06/2017
14	Main Document and all Appendices (1) Updated ARS references to MAC ARS (2) Added section 3.14/MAC ARS Control Tailoring (3) Added section 3.15/Data Loss Prevention (4) Added section 3.16/Wireless Access Monitoring (5) Added section 3.17/ Malicious Software (6) Added section 3.18/Whitelisting (7) Added section 3.19/Data Encryption (8) Updated Attachment 1/MAC ARS	02/2018
15	*Multiple changes have been made to the document* (1) Late addition: Added Section 3.9 on Identity Proofing (2) Updated various sections and language throughout	*05/2022*

CMS/Business Partners
Systems Security Manual

Table of Contents

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Table of Contents

Appendices

Appendix A Medicare Information Technology (IT) Systems Contingency Planning

Appendix B An Approach to Fraud Control

Attachments

Attachment 1 Medicare Administrative Contractor Acceptable Risk Safeguards

1 - Introduction

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements

This manual addresses the following key Medicare Fee For Service business partner security elements:

- A business partner is a contractor involved in Medicare fee-for-service claims processing
- An overview of primary roles and responsibilities
- A program management planning table to assist System Security Officers (SSOs) and other security staff in coordinating system security programs at business partner sites
- The collection of CMS policies, procedures, standards, and guidelines can be found on the CMS Information Security Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html
- The specific version of the ARS to be used by the Medicare Administrative Contractors (MAC) is the MAC ARS, which is Attachment A of this document.
- As the MACs are designated High Value Assets (HVAs), the CMS designated controls for HVA systems are required to be implemented.

The Centers for Medicare and Medicaid Services (CMS) provides health coverage to more than 100 million people through Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplace. As a Federal agency, the systems used to process data are required to follow the Federal Information Security Modernization Act (FISMA) of 2014.

FISMA defines three security objectives for information and information systems: Confidentiality, Integrity and Availability (CIA). FISMA also directs the promulgation of Federal standards for: (i) the security categorization of Federal information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; and (ii) minimum security requirements for information and information systems in each such category. These Federal standards are issued in the form of Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, and FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, respectively.

Using FIPS 199, CMS categorized its information according to information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

For each information type, CMS used FIPS 199 to determine its associated security category by evaluating the potential impact value (e.g., High, Moderate, or Low) for each of the three FISMA security objectives—CIA. The resultant security categorization is the CMS System Security Level.

This is the basis for assessing the risks to CMS operations and assets, and in selecting the appropriate minimum security controls and techniques (i.e., MAC Acceptable Risk Safeguards [ARS] controls).

Federal Information Processing Standards (FIPS) 200 specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. To comply with FIPS 200, agencies shall first determine the security category (i.e., information type) of their information system in accordance with the provisions of FIPS 199, and then apply the appropriate set of baseline security controls contained in the current version of NIST SP 800-53. Recommended Security Controls for Federal Information Systems. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in NIST SP 800-53. This allows agencies, such as CMS, to adjust the security controls to more closely fit its mission requirements and operational environments.

The CMS Information Security and Privacy Policy contains individual policy statements, along with the CMS Minimum Security Requirements, provide technical guidance to CMS and its contractors as to the minimum level of security controls that shall be implemented to protect CMS' information and information systems. These two CMS documents, along with other federal and CMS requirements, are used to form the basis for the CMS ARS.

The "Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) - Section 912: Requirements for Information Security for Medicare Administrative Contractors" (Section 912 of the MMA) provided for a new type of contractor relationship, the "Medicare Administrative Contractor (MAC)," and implemented requirements for annual evaluation, testing, and reporting on security programs at both MACs and existing carrier and intermediary business partners (to include their respective data centers). In this manual, the terms "business partner" and "contractor" are used interchangeably, and all provisions that apply to business partners also apply to MACs. In addition, the term ARS is used in this manual to mean the ARS that includes the required security and privacy control baselines and tailored with the supplemental controls identified by the Business Owner and Information System Security Officer (ISSO). For the MACs, this will be known as the MAC ARS.

CMS requires that the MACs, the primary CMS Medicare claims processing business partner, implement information security controls on their information technology (IT) systems to maintain the CIA of Medicare systems operations in the event of computer incidents or physical disasters.

A sound entity-wide security program is the cornerstone of effective security control implementation and maintenance. Security controls cannot be effective without a robust entity-wide security program that is fully sponsored and supported by senior management, and staffed by individuals with proper training and knowledge.

1.1 - Additional Requirements for MACs

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

MACs are responsible for fulfilling all existing business partner requirements. Additional requirements include the following:

- The contractor shall comply with the CMS MAC tailored list of controls found in Attachment 1. This list of controls, known as the MAC ARS, includes all of the CMS required controls plus optional controls are included specifically for the MACs. MAC ARS controls will be tailored via the BPSSM as what is included in the BPSSM overrides the MAC ARS controls with the intent of being more restrictive.

- The contractor shall correct weaknesses, findings, gaps, or other deficiencies within 90 days of receipt of any final audit or evaluation report, unless otherwise authorized by CMS. If additional time is required, a milestone to implement mitigating controls must be documented prior to requesting the additional time. If the report is related to a required HVA assessment, the contractor shall correct findings in accordance with CISA remediation requirements.

- The contractor shall document system security controls in the CMS FISMA Controls Tracking System (CFACTS) tool to demonstrate compliance with MAC ARS controls and documentation. The contractor shall also use CFACTS to maintain documentation that supports the Authority to Operate (ATO) process, including certification of the documentation.

- The contractor shall conduct or undergo an independent security control assessment of its system security program in accordance with Section 912 of the MMA. The first test shall be completed before the contractor commences claims payment under the contract.

- The contractor shall appoint a Chief Information Officer (CIO) to oversee its compliance with the CMS information security requirements. The contractor's principal Systems Security Officer (SSO) shall be a full-time position dedicated to assisting the business partner CIO in fulfilling these requirements.

- The contractor must implement systems in a manner that is compliant with the CMS Target Lifecycle (TLC) and the Technical Reference Architecture (TRA). When directed by CMS, compliance with the TLC and the TRA will be demonstrated by presenting system updates to the CMS Technical Review Board (TRB). For situations where the TRA conflicts with the MAC ARS, the MAC ARS shall take precedence.

- The contractor shall meet all contingency planning and disaster recovery requirements included in the MAC ARS and the Business Partners Systems Security Manual (BPSSM), with the goal of restoring key claims processing and operations within 72 hours.

- The contractor shall review, update and approve all policies and procedures every 365 days and not every three years as stated in the MAC ARS.

2 – Information Technology (IT) Systems Security Roles and Responsibilities

2.1 - Key Personnel Roles

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements
Business partners shall designate a principal (i.e., primary) SSO who is qualified to manage the Medicare information security program and ensure the implementation of necessary safeguards. The SSO shall be organizationally independent of IT operations. The SSO can be within the CIO organizational domain but cannot have responsibility for operation, maintenance, or development.

See Section 1.1 for additional requirements that pertain to the Medicare Administrative Contractor SSO position.

The business partners that process Medicare data shall maintain an Authority to Operate (ATO) for the information technology systems that are used. The ATO requires that certain roles be filled by Federal personnel and other roles to be filled by business partner personnel. Many of the roles, and the associated responsibilities, are listed in the CMS Information Systems Security and Privacy Policy (IS2P2) and the HHS Information Systems Security and Privacy Policy (IS2P)[1] manuals. Some of the key personnel listed in the IS2P2 include:

- Business Owner (BO)
- Contracting Officer Representative (COR)
- Information System Security Officer (ISSO)
- System Developer Maintainer (SDM)

In addition to the above roles, the business partner personnel shall include a principal System Security Officer (SSO). The SSO position for each contractor should be full-time and fully qualified—preferably credentialed in systems security (e.g., Certified Information Systems Security Professional [CISSP]). Having an individual with appropriate education and experience to execute security administration duties will help reinforce that security must be a cultural norm that guides daily activities, and not a set of compliance directives. A qualified SSO who is available to direct security operations full-time provides the foundation for the security culture and awareness of the organization. The SSO should also encourage their systems security personnel to pursue security accreditation using available funding.

A business partner may have additional SSOs at various organizational levels, but all security actions that affect Medicare operations shall be coordinated through the principal SSO. The SSO ensures compliance with the CMS information security program and MAC ARS by:

- Facilitating the Medicare IT system information security program and ensuring that necessary safeguards are in place and working

- Coordinating information security system activities throughout the organization

[1] The HHS IS2P document is available by requesting it from your Federal Information System Security Officer

- Ensuring that IT system information security requirements are considered during budget development and execution

- Reviewing compliance of all components with the MAC ARS and reporting vulnerabilities to management

- Ensuring an incident response capability is established for investigating system security and privacy breaches and reporting significant problems (see section 3.6) to business partner management and CMS.

- Ensuring that technical and operational information security controls are incorporated into new IT systems by participating in and reviewing all new systems/installations and major changes

- Ensuring that IT systems information security requirements are addressed in Requests for Proposal (RFP) and subcontracts involving the handling, processing, and/or analysis of Medicare data

- Maintaining information security documentation in the System Security Profile for review by CMS and external auditors and keeping all elements of the System Security Profile (see section 3.7)

- Cooperating in all official external evaluations of the business partner's information security program

- Facilitating the completion of the Information Security Risk Assessment (see section 3.2)

- Ensuring that an operational IT Systems Contingency Plan (ITSCP) is in place and tested (see section 3.3)

- Documenting and updating the monthly Plan of Action and Milestones (POA&M) (see section 3.5.2). Updates may occur whenever a POA&M scheduled completion date passes, and/or following the issuance of new requirements, risk assessments, internal audits, and external evaluations.

- Ensuring that appropriate safety and control measures are arranged with local fire, police, and health agencies for handling emergencies (see Appendix A)

The principal SSO shall earn a minimum of 40 hours in continuing professional education credits each year. The educational sessions conducted at the CMS Security Controls Oversight and Update Training (CSCOUT) can be used toward fulfilling the continuing professional education credits. The associated credit hours will be noted on the CSCOUT agenda.

2.2 – Personnel Security/Suitability

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

All business partner and contractor personnel requiring access to CMS sensitive information shall meet minimum personnel suitability standards. These suitability standards are based on a valid need-to-know (not based on position or title) and favorable results from a background check. Each position must be evaluated and assigned a risk and/or a sensitivity designation commensurate with each individual's duties and responsibilities. The background check for prospective employees shall include, at a minimum: Social Security Number verification, identity and address verification, national criminal database search, county criminal records search, HHS list of excluded individuals, sex offender registry, verification of academic records when required for the position and verification that the employee has resided in the US for 3 of the past 5 years.

When required by CMS, business partner personnel will need to complete a Federal Background Investigation (BI). To initiate a BI, business partner personnel will need to supply personal information to CMS via methods (fingerprint card) or systems identified by CMS. The level of investigation for a BI varies and will be determined by the COR's risk assessment of the person's role. A BI that results in a favorable outcome can result in a Personal Identity Verification (PIV) card being issued.

3 - IT Systems Security Program Management

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements
The Security Program consists of several fundamental components that are all designed to implement controls and to reduce risk. Key elements of controls include Policies, Procedures, Technical Implementations, Standards, and Management Reviews.

Required security documentation includes, but is not limited to, the system security plan, the information security risk assessment, and the IT systems contingency plan.

Business partners shall implement an IT Systems Security Program to manage the system security risks. Risks are identified by the business partner in the Information Security Risk Assessment (see section 3.2) and the security requirements are documented in the System Security Plan (see section 3.1). The underlying support for these documents is the controls implemented by the business partner. Information system security controls shall be implemented in a consistent manner everywhere within the system's accreditation boundary to protect the CIA of sensitive information. In addition, testing shall be performed to ensure that information security controls are operating as intended.

3.01 - Control Components

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Business partners shall have policies and procedures, and implement controls or plans that fulfill the MAC ARS controls. The business partner Medicare claims related security program shall be based on the MAC ARS (IOM 100-17, Attachment 1), the BPSSM (IOM 100-17) and on the collection of CMS policies, procedures, standards, and guidelines found on the CMS Information Security Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html.

Policies are formal, up to date, documented rules that are tailored to the environment, are communicated as "shall" or "will" statements and are readily available to employees. They establish a continuing cycle of assessing risk, implementing controls and monitoring for program effectiveness. Policies are written to cover all major facilities and operations corporate-wide or for a specific asset (e.g., Medicare claims processing), and they are approved by key affected parties. Policies delineate the IT security management structure, clearly assign IT security responsibilities, and lay the foundation necessary to reliably measure progress and compliance. Policies also identify specific penalties and disciplinary actions to be used in the event that the policy is not followed.

Procedures are formal, up to date, documented instructions that are provided to implement the security controls identified by the defined policies. They clarify where the action is to be performed, how the action is to be performed, when the action is to be performed, who is to perform the action, and on what the action is to be performed. Procedures clearly define IT security responsibilities and expected behaviors for: asset owners and users, information resources management and data processing personnel, management, and IT security administrators. Procedures also indicate appropriate individuals to be contacted for further information, guidance, and compliance. Finally, procedures document the implementation of, and the rigor with which, the control is applied.

Technical Implementations are the acquisition and installation of hardware, software, or assets to be used for the establishment of a new control, or the improvement of an existing control. The intention of a technical implementation is to automate or facilitate a control process that would otherwise be manually performed.

Standards are formal, written, mandatory actions, rules, or specifications designed to support and conform to a policy or procedure. A standard must include one or more accepted specifications for configurable items for hardware, software, or behavior. Standards are often required to successfully complete technical implementations and can be either part of policies and procedures, or can be standalone documents. Standards can result from, either exclusively by or in combination with, laws promulgated by governing bodies, obtained from known standards organization or developed by the business partner using industry best practices.

Management Review is the business partners' formal oversight activity of control implementations and should be performed at various management levels. Oversight is a regular activity to verify that the control environment for which management has responsibility is functioning properly. Management must set benchmarks or other methods to measure the success of controls. Where appropriate, management should document their review by formally approving evidence supplied.

3.02 - Reporting Requirements

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements
Business partners are required to provide documentation to CMS regarding the status of their IT security program. Documentation shall be reported to CMS according to the appropriate procedures, which are summarized in Table 3.1.

Meeting requirements does not validate the quality of a program. Managers with oversight responsibility shall understand the processes and methodology behind the requirements. Table 3.1 identifies key requirements and their high-level descriptions. As appropriate, Table 3.1 refers to other parts of this document that provide details on ways to accomplish each requirement.

In addition, Table 3.1 indicates how often these requirements need to be performed, the disposition of output or documentation, comments, and a space to indicate completion or a "do by" date. The number accompanying each entry in the requirement column indicates the section in this document that deals with that particular requirement. Use this table as a checklist to ensure that all required IT systems security tasks are completed on schedule. Consult the referenced sections for clarifying details.

Table 3.1. Reporting Requirements Planning Table

Requirement	Frequency	Send To	Comments	Complete (check when complete)
System Security Profile – Section 3.7	As necessary	• On file with the Principal SSO	The System Security Profile documents may be stored as paper documents, electronic documents, or any combination thereof.	

Requirement	Frequency	Send To	Comments	Complete (check when complete)
CMS Annual FISMA Assessment (FA) – Section 3.5.1	One third of the controls shall be tested each year so all controls are tested during a 3-year period.	• COR with a copy to CMS CO via CFACTS • System Security Profile	FA results recorded in the CFACTS are to be discussed in the Certification Package for Internal Controls (CPIC).	
System Security Plan (SSP) – Section 3.1	The SSP for each General Support System (GSS) and MA shall be reviewed, updated, and approved by management every 365 days, or upon significant change[2].	• CMS CO via CFACTS • System Security Profile	Information system security plans are to be generated via CFACTS, reviewed, updated, and approved by management and the approved SSP saved in CFACTS, the CPIC and Statement of Certification, and the System Security Profile.	
Information Security Risk Assessment – Section 3.2	The information security risk assessment for each GSS and MA shall be reviewed, updated, and approved by management every 365 days, or upon significant change.[1]	• CMS CO via CFACTS • System Security Profile	Information security risk assessments are to be reviewed, updated, and approved by management and saved in the CFACTS, the CPIC and Statement of Certification, and the System Security Profile. The information security risk assessment is submitted with the system security plan[3].	
Certification (CPIC) – Section 3.4	Each federal FY	• COR with a copy to CMS CO via CFACTS • System Security Profile	Business Partners should include a statement of certification as part of their CPIC. Each year CMS will publish in Chapter 7 (Internal Controls) of its Financial Management Manual (Pub 100-06) information on certification requirements including where, when, and to whom these certifications shall be submitted. All other contractors should submit a statement of security certification to their CMS CORs.	
IT System Contingency Planning – Section 3.3	CPs shall be reviewed, updated, and approved by management every 365 days, or upon significant change.[1] CPs shall be tested annually.	• CMS CO via CFACTS • System Security Profile	Business partner management and the Business Owner shall approve the CP. The ITSCP is to be developed (in accordance with Appendix A and CMS RMH documents), reviewed, updated, and approved by management—and saved in CFACTS, the Certification Package/Statement of Certification, and the System Security Profile[4].	
Plan of Action and Milestones – Section 3.5.2	Each federal FY	• ISSO • COR • CMS CO via CFACTS • System Security Profile	POA&Ms address findings of internal/external audits/reviews including annual security assessments, and, as applicable: Statements on Standards for Attestation Engagements (SSAE) 18 reviews, A-123, Chief Financial Officer (CFO) controls audits, the Section 912 evaluation, and data center tests and reviews.	

[2] NIST defines “significant change” as “any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets.”

[3] More information about Risk Assessment Reports can be found in the CMS risk assessment procedures.

[4] More information about contingency planning can be found in NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, and NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems.

Requirement	Frequency	Send To	Comments	Complete (check when complete)
Incident Reporting and Response – Section 3.6	As necessary	• COR • CMS IT Service desk • Medicare Contractor Management Group (MCMG) Security Mailbox (See the latest guidance from CMS for more information) • System Security Profile	Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH) and the Privacy Act of 1974 addresses Incident Reporting information.	
Authorization To Operate – Section 3.8	As necessary to acquire and maintain a CMS CIO-granted Authorization to Operate.	On file with CMS Information Security and Privacy Group (ISPG), with a copy maintained in the CFACTS.		

TABLE 3.1 LEGEND:

CFACTS	CMS FISMA Controls Tracking System
CFO	Chief Financial Officer
CO	Central Office (CMS)
COR	Contract Officer Representative
ITSCP	IT System Contingency Plan
CPIC	Certification Package for Internal Controls
FA	FISMA Assessment
FY	Fiscal Year
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
MA	Major Application
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SSAE	Statement on Standards for Attestation Engagements
SP	Special Publication (NIST)
SSO	Business Partner Systems Security Officer

When submitting documentation to the CMS Central Office, Registered Mail™ or its equivalent (signed receipt required) shall be used. Contact the appropriate COR or ISSO for the correct address.

3.1 - System Security Plan (SSP)

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements
Business partners are required to update and re-certify the SSP every 365 days unless there are changes that would necessitate a more frequent update. Updates to the SSP shall be performed via CFACTS.

Defining a system boundary is a key step that must be completed before a SSP can be accurately documented.

The SSP should address how the control environment is implemented to mitigate risks identified in the information security risk assessment.

The objective of an information security program is to improve the protection of sensitive/critical IT resources. All business partner systems used to process, transmit, or store Medicare-related data have some level of sensitivity and require protection. The protection of a system shall be documented in a SSP. The completion of a SSP is a requirement of the Federal Information Security Management Act of 2014 (FISMA), Privacy Act of 1974, As Amended, Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, the Computer Security Act of 1987. All Medicare claims-related applications and systems categorized as either an MA or GSS shall be covered by SSPs.

The purpose of a SSP is to provide an overview of the security requirements of a system and describe the controls that are implemented to meet those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. The SSP should be viewed as documentation of the structured process of planning adequate and cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including Business Owners, information owners, the system operator, and the system security manager (i.e., SSO).

All business partners are required to maintain current security plans for their Medicare claims-related GSSs and MAs in both the CFACTS and their System Security Profiles. The SSP documents the current level of security within the system or application; that is, actual implemented controls, not planned controls. In addition, the SSP serves as the primary documentation reference for testing and evaluation, whether by CMS, the General Accounting Office (GAO), or other oversight bodies. The SSP is a sensitive document, as it may discuss uncorrected vulnerabilities and may mention risks that have been accepted. Therefore, security plans should be distributed only on a need-to-know basis.

The SSP shall be recertified by business partner management and the signed copy made available to the SSO and authorized external auditors as required. The SSO and business partner are responsible for reviewing the SSP on an annual basis to ensure that it is up to date. The objective of these annual reviews is to verify that the controls selected or installed remain adequate to provide a level of protection to reach an acceptable level of risk to operate the system.

All business partner Medicare claims-related SSPs shall be developed and documented in accordance with the latest instruction from CMS.

SSP shall be recertified within 365 days from the previous certification date. The SSP shall also be reviewed prior to recertification (within the original certification timeframe) to determine whether an update is required. The SSP shall be updated if there has been a significant change or the security posture has changed. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review or the updated SSP, if applicable, shall be documented in the CFACTS, and placed in the System Security Profile.

Contractors updating their current security plan(s) or developing new security plan(s) shall take into account Medicare claims processing front-end, back-end, and/or other claims processing related systems.

Front-end systems are those systems Medicare contractors develop and maintain for use in their operations areas and data centers to enter claims and claims-related data into the standard/shared claims processing system. These front-end systems include, but are not limited to: electronic data interchange, imaging systems, optical character recognition, manual claims entry, claims control, provider, beneficiary, other payer databases, and other pre-claims processing business functions.

Back-end systems are those systems that Medicare contractors develop and maintain for use in their operations areas and data centers to output claims processing information (i.e., checks, Medicare summary notices, letters, etc.). These back-end systems include, but are not limited to: print mail, 1099 forms, post-payment medical reviews, customer service, appeals, overpayment written/phone inquiries and separate claims reconciliation systems.

Within 10 business days of updating, developing or recertifying an SSP, CFACTS must be updated.

3.2 – Information Security Risk Assessment (ISRA)

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements

Business partners are required to perform an annual ISRA in accordance with the most current versions of the CMS ISRA procedures available on the CMS Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html. The identified risks will aid in the design of controls to satisfy the MAC ARS.

Documentation of the risks needs to be completed before a control is designed and implemented. Controls should be designed to be cost effective based on the risk to the operating environment.

Risks never go away, but can increase as new vulnerabilities are found and decrease as new or enhanced controls are implemented.

The CMS procedures present a systematic approach for the ISRA process for Medicare information computer systems within the CMS and business partner environments. The procedure describes the steps required to produce an ISRA for systems and applications.

All business and information owners shall develop, implement, and maintain risk management programs to ensure that appropriate safeguards are taken to protect all CMS resources. A risk-based approach shall be used to determine adequate security and shall include a consideration of the major factors in management, such as the value of the system or application, all threats, all vulnerabilities, and the effectiveness of current or proposed safeguards. The CMS risk assessment procedures shall be used to prepare an annual ISRA.

ISRAs shall be recertified within 365 days from the previous certification date. The ISRA shall also be reviewed prior to recertification (within the original certification timeframe) to determine whether an update is required. The ISRA shall be updated if there has been a significant change or the security posture has changed. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review or the updated ISRA, if applicable, shall be placed in the System Security Profile, and a copy shall be submitted to the CMS Central Office. Note that the ISRA used to support a security plan cannot be dated more than 365 days earlier than the security plan certification date.

Contractors that must update their current ISRA shall use the most current versions of the CMS procedures and templates.

A newly developed or updated ISRA that is submitted with the security plan shall be maintained in the CFACTS within 10 working days after they have been developed and/or updated.

The ISRA shall be updated every 365 days unless there are changes (as discussed above) that would necessitate a more frequent update. Should ISRA technical assistance be required, direct all questions to the CMS Information Security and Privacy Group (ISPG) at mailto:CISO@cms.hhs.gov.

Technical Limitations - In the event that a technical limitation prevents compliance with an ARS control, MACs should consult with CMS and the guidance for documenting a Technical Limitation Acknowledgement (TLA). If possible, the related control or configuration should be set as restrictive as possible.

3.3 – IT Systems Contingency Plan (ITSCP)

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements
Business partners are required to document and test an ITSCP in accordance with the most current versions of the CMS Information Security Contingency Planning standards and procedures available on the CMS Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html, and with BPSSM Appendix A.

All business partners are required to develop and document an ITSCP that describes the arrangements that have been implemented and the steps that shall be taken to continue IT and system operations in the event of a natural or human-caused disaster. The ITSCP shall be included in management planning and shall be:

- Reviewed as part of a documented System Development Life Cycle, whenever new systems are planned or upon significant change

- Reviewed when new safeguards are implemented

- Reviewed and approved within 365 days to ensure accuracy

- Tested within 365 days. If backup facility testing is done by Medicare contract type (i.e., when multiple contract types are involved [e.g., Data Center, Part A/B, DME]), each individual Medicare contract type shall be tested every 365 days.

Updated plans and test reports (results) shall be maintained in CFACTS, and placed in the contractor's System Security Profile. Business partner management and the SSO shall approve newly developed and/or updated ITSCPs. A newly developed and/or updated IT Systems CP shall be updated in CFACTS and submitted to CMS within 10 business days after the business partner's management and SSO have approved it.

Appendix A to this manual provides information on ITSCP and testing methods. Also, see Table 3.1 for additional information.

3.4 – Certification Package for Internal Controls (CPIC)

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

All business partners are required to certify their system security compliance. Certification is the formal process by which a contractor official verifies, initially and then by annual reassessments, that a system's security features meet the MAC ARS controls. Business partners shall self-certify that their organization successfully completed an annual, independent FA of their Medicare IT systems and associated software in accordance with the terms of their Medicare agreement/contract.

Each contractor is required to self-certify to CMS its information security compliance within each federal Fiscal Year (FY). This security certification shall be included in the CPIC or, for contracts not required to submit CPICs, send the security certification to their appropriate CMS CORs. CMS shall continue to require annual, formal re-certifications within each FY no later than September 30, including validation at all levels of security as described in this manual.

System security certification shall be fully documented and maintained in the System Security Profile. The security certification validates that the following items have been developed (i.e., updated and/or reviewed, as required) and are available for review in the System Security Profile:

- Certification

- FISMA Annual Security Control Assessment

- System Security Plan for each GSS and MA (see section 3.1)

- Information Security Risk Assessment (see section 3.2)

- IT Systems Contingency Plan (see section 3.3 and Appendix A)

- Plan of Action and Milestones (see section 3.5.2)

3.5 - Compliance

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Compliance refers to the contractual obligations of business partners to CMS. The components to comply with IT security requirements are described in detail in the following subsections.

3.5.1 - Annual FISMA Assessment (FA)

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements
At least 1/3 of controls must be tested each year, and all controls shall be tested over a 3 year period.

CMS identifies which control families must be tested each year.

A critical factor for maintaining on-going compliance with FISMA and the Federal Managers' Financial Integrity Act of 1982 (FMFIA) is for Business Owners in coordination with developers/maintainers, to annually test their internal controls and dedicate sufficient resources to accomplish this test. These resources include budget (if external resources are to be used to support the testing) and person-hours (if internal personnel are to be engaged in this activity). They are required to schedule and perform the test; and oversee the development and completion of applicable POA&Ms for vulnerabilities noted during the annual testing.

The annual FA is documented, tracked, and reported in the CFACTS. The purpose of annual FA testing (i.e., validation) is to examine and analyze implemented security safeguards in order to provide evidence of compliance with applicable laws, directives, policies, and requirements regarding information security. The annual FA is intended to validate the MAC ARS controls to determine the extent to which the controls are:

- implemented correctly
- operating as intended
- producing the desired outcome with respect to meeting the security requirements for the system

The annual FA testing requirement has been interpreted by OMB as being within 365 calendar days of the prior test. Over a 3-year period, all MAC ARS controls applicable to a system or application shall be tested. This means a subset (no less than one-third [$^{1}/_{3}$]) of the MAC ARS controls shall be tested each year so that all security controls are tested during a 3-year period. In an effort to standardize testing and results summarization, a 3-year rotation of MAC ARS control families was established by CMS. After the 3-year rotation is completed, the testing rotation shall be repeated until notification from CMS is received. As control families are added or removed, CMS reserves the right to change the controls that must be tested each year.

To fulfill the annual FA validation obligation, the FA shall be conducted by an independent agent or team. This can be any internal/external agent or team that is capable of conducting an impartial assessment of an organization's information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management chain of command associated with the information system or to the determination of MAC ARS effectiveness. All management-directed and independent testing conducted within 365 days of the attestation due date may be used to meet the requirement for the annual security controls (i.e., FA) testing.

3.5.2 - Plan of Action and Milestones (POA&M)

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements
Business partners are required to prepare a monthly POA&M update which is due by the 1st of each month. The POA&M update consists of updating all active POA&Ms in the CFACTS and, if required by CMS, uploading any additional supporting documentation.

All security and privacy related findings shall be entered into CFACTS. This includes findings from Section 912, FISMA, CFO, security control assessments, penetration tests, Statement on Standards for Attestation Engagement No. 18 (SSAE-18) and all other reviews and audits.

3.5.2.1 - Background

FISMA requires that federal agencies provide annual reporting of the state of security programs for all IT systems associated with the agency. Additionally, periodic POA&Ms reporting the status of known security weaknesses for all federal agency systems are also submitted to the OMB. This reporting requirement applies to a broader scope of security weaknesses, as it is not limited to weaknesses identified by specific audits and reviews (such as those covered under FMFIA). In the case of FISMA, any security weakness identified for any covered system shall be recorded in CFACTS.

Section 912 of the MMA implemented requirements for annual evaluation, testing, and reporting on security programs for MAC business partners (to include their respective data centers). These Section 912 evaluations and reports necessitate an annual on-site review of business partner security programs to ensure that they meet the information security requirements imposed by FISMA and CMS. CMS, as part of its overall FISMA reporting obligations, requires that corrective actions for identified deficiencies (i.e., weaknesses) be addressed in a report to be submitted shortly after the evaluation results are finalized, as well as periodically thereafter to track updated progress towards completion of the identified action plans.

The CFACTS enables contractors to satisfy reporting requirements for security and privacy related findings. Security and privacy related findings and approved action plan data is promptly entered into the CFACTS following all audits/reviews.

3.5.2.2 - POA&M Components/Submission Format

(Rev. 11, Issued: 09-30-11, Effective: 10-31-11, Implementation: 10-31-11)

The CFACTS shall be populated and maintained with security and privacy related findings and action plans from any audit or review, whether internal or external. Corrective actions are to be established in the CFACTS to address all resulting weaknesses entered therein, and those corrective actions shall be maintained current in the CFACTS to support reporting requirements. In addition to the initial POA&M reporting that follows each audit/review, ongoing milestones for all corrective action plans will be updated on the 1st business day of each month.

Initial Reporting. Within 30 calendar days (or as otherwise directed by CMS) of the final results for every internal/external audit/review, an initial POA&M is due to CMS that describes the findings of the audit/review and initial corrective actions planned for implementation.

Monthly Reporting. On a monthly basis, business partners shall provide updates in the CFACTS on progress towards completion of remediation efforts for weaknesses identified from all known sources.

3.5.3 - Timing Requirements for Compliance Conditions

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

In the MAC ARS, many security documents and processes require timely execution on a yearly, bi-annual (every 6 months), quarterly, monthly, weekly or daily basis. In order to assure that these documents/processes are reviewed/processed timely, the following timing requirements apply:

- Yearly/365 days: Any document/process to be reviewed on a yearly basis shall be performed within the same month each year. For example, if you review your ISRA or ITSCP on February 14th, then the next review must take place within the month of February during subsequent years. This can be applied to reviews to be performed over multiple years. If you perform a review in February and a review is due 3 years later, it must be performed within the month of February for the year when the review is to be performed again. The only exceptions to this annual/yearly compliance condition are deliverables whose annual due date are set and distributed by CMS, such as the annual FA submission.

- Bi-Annual/Every 6 Months/180 days: The months designated for a 6-month document/process review shall occur every 6 months and be consistent from year to year. For example, if you perform an initial review during February, then the next review must be performed within the month of August. In subsequent years, the review must be performed within the months of February and August. Those months then become your standard months for performing the review.

- Quarterly/90 days: The months designated for a quarterly document/process review shall occur every 3 months and be consistent from year to year. A quarterly document/process review shall be scheduled on the same day of each designated month and be performed within 4 business days** before or after the scheduled review date of those months. That is, if you choose July 16 as your review date, then your review date will be the 16 in each designated month. The following table demonstrates when quarterly reviews must be performed based on the day your scheduled review date occurs.

Earliest Review	Review Target Day	Latest Review
Previous Tuesday	Monday	Following Friday
Previous Wednesday	Tuesday	Following Monday
Previous Thursday	Wednesday	Following Tuesday
Previous Friday	Thursday	Following Wednesday
Previous Monday	Friday	Following Thursday

  **Federal holidays or incidental office closures will not affect these timeframes.

- Monthly/30 days: The document/process review shall be performed within 2 business days** before or after the scheduled review date each month. The exact date of the monthly review shall not change month to month. That is, if you choose July 16th as your review date, then your review date will be the 16th in every subsequent month. The following table demonstrates when monthly reviews must be performed based on the day your scheduled review date occurs.

Earliest Review	Review Target Day	Latest Review
Previous Thursday	Monday	Following Wednesday
Previous Friday	Tuesday	Following Thursday

Previous Monday	Wednesday	Following Friday
Previous Tuesday	Thursday	Following Monday
Previous Wednesday	Friday	Following Tuesday

**Federal holidays or incidental office closures will not affect these timeframes.

- Weekly/7 days: Weekly/7 days document/process reviews shall be performed on the same day every week. If the scheduled review day falls on a holiday, the previous or subsequent business day can be used as your review target date, returning to the original target date in subsequent weeks.

- Daily/24 hours: Daily/24 hours document/process reviews shall be performed on the next business day. If the day of the scheduled review falls on a Saturday, then the review is performed on a Monday. If the day of the scheduled review falls on a federal holiday or an incidental office closure, then the review is performed the next business day. This may cause more than one review to be performed on the same day.

If the business partner wishes to change the timing cycle of a review, the business partner is required to shorten the timing cycle and not lengthen the timing cycle to attain the new performance date. For example, if the annual/yearly review of the security plan is being performed in June during year 1 and the business partner desired to change the review date for year 2, they would be required to review the security plan in a month prior to June. That month would then become the review month going forward.

Exceptions to the timing requirements can be implemented with the approval of the CMS ISSO. These can be one-time exceptions (e.g., a yearly review of a disaster recovery test is performed after an established month due to scheduling issues with the recovery facility).

3.6 - Security Incident Reporting and Response

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements
All security incidents shall be reported to CMS in accordance with the requirements listed in the CMS Risk Management Handbook (RMH) Chapter 8. Incidents shall be reported to the IT Service Desk. A security incident is a PII or PHI breach, a ransomware event, or an event that impacts the confidentiality, integrity or availability of Medicare data.

MACs shall also email each incident report to mailto:Security_Incident@cms.hhs.gov.

NIST Special Publication 800-61r2 defines a computer security incident as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.

- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

An “imminent threat of violation” refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of new malware that is rapidly spreading across the Internet.

The business partner shall use its security policy and procedures to determine whether a non-reportable event or a reportable security incident has occurred. Examples of non-reportable events include a user connecting to a file share, a server receiving a request for a web page, a user sending email or a firewall blocking a connection attempt. Upon receiving notification of an IT systems security incident or a suspected incident, the SSO or another identified individual shall immediately perform an analysis to determine if an incident actually occurred. The incident should be evaluated to determine if it impacts the processing of Medicare data or the confidentiality, integrity and availability of Medicare data.

All suspected security incidents or events shall be reported to the business partner’s IT service desk (or equivalent business partner function) as soon as an incident comes to the attention of an information system user. All security incidents and events shall be reported to the CMS IT Service Desk in accordance with the procedures set forth in the CMS RMH Chapter 8 Incident Response. This document is available on the CMS Information Security Web site at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html. The CMS IT Service Desk can be contacted by telephone at 800-562-1963 or 410-786-2580, or by e-mail at: mailto:CMS_IT_Service_Desk@cms.hhs.gov. Contacting the CMS IT Service Desk by telephone is recommended if immediate action by CMS is required. In addition, MACs shall also email each incident report to mailto:Security_Incident@cms.hhs.gov .

When reporting confirmed security incidents, business partners shall report the date and time when events occurred or were first discovered; names of systems, programs, or networks affected by the incident; and impact analysis. Release of information during incident handling shall be on an as-needed and need-to-know basis. When other entities should be notified of incidents at external business partner sites, CMS will coordinate with legal and public affairs contacts at the effected entities. If a violation of the law is suspected, CMS will notify the Office of Inspector General (OIG) Computer Crime Unit and submit a report to the Federal Computer Incident Response Capability (FedCIRC) of the incident with a copy to the CMS CISO.

As part of the risk management process, the business partner shall determine the extent of the incident’s impact and the potential for new or enhanced controls required to mitigate newly identified threats. These new security controls (and associated threats and impacts) should provide additional input into the business partner’s ISRA. Business partners shall refer to CMS RMH Chapter 8 Incident Response manual for further guidance.

Many of the PII breaches being reported to CMS occur when unencrypted emails are sent to the intended recipients. A mitigating control to allow many of these breaches to be closed more easily is the implementation of the Transport Layer Security (TLS) protocol within email servers such as Microsoft Exchange. The TLS protocol encrypts emails for transmission between two email servers. There are different TLS features which can be used and provide different levels of assurance that an email will be encrypted. Use of any of these features requires TLS to be enabled. To mitigate the severity of email PII breaches, business partners are required to enable TLS on their email servers. In addition, the most secure TLS feature that can be enabled to encrypt emails between business partners shall be implemented. If a business partner cannot implement TLS, a risk must be documented in the RA.

3.7 - System Security Profile

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements
The System Security Profile is a copy of the documents that are maintained in CFACTS and on CMS Web sites. These documents shall be available if business partner management requires timely access to them without CFACTS or CMS Web site availability.

Consolidate security documentation (paper documents, electronic documents, or a combination) into a System Security Profile that includes the following items:

- Completed FAs
- Security Plans (for each GSS and MA)
- Risk Assessments
- Certifications
- Contingency Plans
- POA&Ms for each compliance security review
- POA&Ms for other security review undertaken by Department of Health and Human Services (HHS) OIG, CMS, Internal Revenue Service (IRS), GAO, consultants, subcontractors, and business partner security staff
- Incident reporting and responses
- Systems information security policies and procedures

The System Security Profile shall be kept in a secure location, kept up to date, and pointers to other relevant documents maintained. A backup copy of the System Security Profile shall be kept at a secure off-site storage location, preferably at the site where back-up tapes and/or back-up facilities are located. The back-up copy of the profile shall also be kept up to date, particularly the contingency plan documents.

3.8 - Authorization To Operate

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Business partners are required to acquire and maintain a CMS CIO-issued Authorization to Operate (ATO) for each FISMA system. To maintain an ATO, the business partner is expected to maintain all security documentation in CFACTS, and the documentation must be up to date as defined in BPSSM table 3.1. When applying for an ATO, critical and high risk POA&Ms must be in either a pending verification status or mitigated so the risk can be demonstrated to be moderate or low.

3.9 – Identity Proofing

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements
Identity proofing establishes that a user (both organization or non-organizational) is who the user claims to be. Identity proofing is the process of collecting, validating, and verifying user's identity information for the purposes of issuing credentials for accessing a system.

Assuring appropriate identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries.

Care should be taken to ensure that only the absolute necessary information be obtained in order to keep the amount of PII that is collected to a minimum.

Business partners shall assure that users are effectively identity proofed in accordance with ARS control requirements. To assure that users are properly identified and validated, it is imperative that business partners apply consistent identity proofing concepts.

To properly identity proof users, business partners shall implement a process that meets the requirements identified within NIST 800-63A and meets or exceeds standards for IAL2.

It is not a requirement that identity proofing be done in person.

Exceptions and situations that require further clarification should be discussed with CMS before implementing.

3.10 - Patch Management

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements
The timely patching of systems is one of the critical controls to preventing network intrusions.

The MAC ARS requires the correction of identified security-related information system flaws on production equipment based on a frequency / time frame documented in the applicable system's patch management plan. The time frame begins when the vendor releases a patch, not when the business partner becomes aware of a patch. The patching requirement is 15 calendar days for all critical patches and 30 calendar days for all other patches.

Timely patching is critical to maintaining the operational CIA of Medicare systems. However, failure to keep operating system and application software patched is the most common mistake made by IT professionals. New patches are released daily and it is often difficult for even experienced system administrators to keep abreast of all the new patches

To help address this growing problem, CMS recommends that business partners have an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches. The MAC ARS provides specific guidance on time frames for implementing patches. Further guidance is provided in Table 3.3 below for 1) Patch Identification, 2) Patch Installation and 3) Unsupported software.

Table 3.3

Patch Identification	Include all patches that are released from the system, application, or device vendor. All patches must be analyzed by the business partner to determine their applicability and security impact on the operating environment. All patches analyzed from the vendor must be tracked through a formal process and categorized as 1) Security or 2) Operational in nature.
Patch Installation	All security patches risk ranked as critical shall be implemented in 15 calendar days. All other security patches, regardless of the patch risk ranking, shall be implemented in 30 calendar days. Security related patches not installed based on business partner analysis shall be documented with an appropriate business justification that includes security impact, operational impact, business impact, mitigating or compensating controls, and residual risk. Re-evaluation of the justification must be performed within every 365 days.
Unsupported Software	Unsupported software, or software that is not formally supported by the software vendor for security or operational patches, shall not be used unless advanced patch support is purchased or provided through another documented source. All unsupported software in operation shall be documented within the Business Partner's ISRA and POA&M with phase out timelines defined. For details, see section 3.12 – End of Life Technology Components.

NIST SP 800-40 Version 3.0, Creating a Patch and Vulnerability Management Program, provides a valuable and definitive process for setting up, maintaining, and documenting a viable patch management process. CMS highly encourages business partners to utilize NIST and other guidance documents to develop configuration standards, templates, and management processes that securely configure Medicare systems as part of their configuration management program.

3.11 - Security Configuration Management

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Key Requirements
Business partners are required to create a security baseline for the configuration of the information system components. A baseline is a formal, management approved standard that documents the customization of Federal or other guidelines.

The process for establishing and maintaining baselines shall allow misconfigurations to be identified and risk-minimized, including a documented process that supports timely resolution of misconfigurations.

Federal guidelines should be used to create baselines. If a Federal guideline does not exist, hardening guides or documented best practices may be used.

DMEMACs, ABMACs, and VDCs are responsible for starting their security configurations with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) Checklists when creating a baseline. All appropriate or referenced DISA checklists and guidelines shall be considered for input into each baseline.

FISMA requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them. CMS requires business partners to utilize guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

Misconfigurations are defined as:

- A setting that violates a configuration policy or that permits or causes unintended behavior that impacts the security posture of a system; or,
- An incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities.

In order to effectively protect MAC environments from vulnerabilities produced by incorrectly configured information system components, any misconfiguration shall be updated/corrected within 30 days from the time of discovery. If the misconfiguration cannot be effectively addressed within that timeframe, a POA&M shall be opened to track and remediate misconfigured setting(s).

Security configuration guidelines may be developed by different federal agencies, so it is possible that a guideline could include configuration information that conflicts with another agency or CMS guideline. To resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing Federal security configuration guidelines follows. If there is a conflict between the MAC ARS and a DISA STIG, the MAC ARS takes precedence. See Table 3.4 for more information. If there are any other questions or concerns about resolving conflicts among security configuration guidelines, business partner SSOs shall contact their CMS ISSO.

Table 3.4

Business Partners	DMEMAC/ABMAC/VDCs
1. MAC ARS 2. United States Government Configuration Baseline (USGCB)	1. CMS/MAC ARS 2. DISA/USGCB

3. NIST National Checklist Program (NCP) / NIST	3. NIST National Checklist Program (NCP) / NIST / Center for Internet Security (CIS)
4. DISA	4. Vendor supplied guidance

3.11.1 - Security Technical Implementation Guides (STIG)

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Security guidelines, called STIGs, are available for most major operating systems, support applications, and infrastructure services. STIGs contain detailed guidance, best practices, and recommendations for configuring a particular product. STIGs are developed by DISA to help system operators configure security within their systems to the highest level possible. DISA also has made available Security Requirement Guides (SRGs) for certain platforms. These guidance documents may be intended to use along with STIGs as the security guidelines for a specific platform. All STIGs and SRGs are available from DISA. The link for these documents is https://public.cyber.mil/stigs/compilations/ . CMS recommends that business partner SSOs (or their designated representative) subscribe to the DISA STIG-News Mailing List at: https://public.govdelivery.com/accounts/USDISA/subscriber/new?topic_id=USDISA_181 so they will be notified whenever updated or new STIG Checklists become available.

The use of latest publicly available DISA STIG is mandatory for all business partner systems/applications that process, store, and/or transmit Medicare claims data. DMEMACs, ABMACs, and VDCs are required to start with the STIG configurations and then document a customized baseline with any deviations based on environment specific implementation. In the event that DISA does not have a STIG available for a specific platform, business partners should follow the defined CMS hierarchy within the MAC ARS controls.

While it may not be possible to implement all of a STIG's recommended security settings because doing so would compromise the functionality of an application and/or system, CMS expects every business partner to analyze the STIG recommended settings and determine which ones are viable, and to implement all settings that are found to be feasible. Settings that cannot be implemented across an entire platform (e.g. Windows 2019, AIX) shall be documented as "system deviations." Customized baseline values (including those that may already be "system deviations") that cannot be implemented on only specific systems shall be documented as "system exceptions,". All STIG recommended security settings that are determined not to be viable in a business partner environment (including "system exceptions") shall be documented in the applicable system/application Security Configuration Checklist (SCC) with appropriate business justification (security impact, operational impact, business impact), mitigating or compensating controls, and residual risk.

3.11.2 - United States Government Configuration Baseline (USGCB) Standard

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration (FDCC) mandate. While not addressed specifically as the FDCC, the process (now coined the USGCB process) for creating, vetting, and providing baseline configurations settings was originally described in a 22 March 2007 memorandum from OMB to all Federal agencies and department heads and a corresponding memorandum from OMB to all Federal agency and department Chief Information Officers (CIO).

Business Partners have the choice of using the USGCB configurations or the STIGs for the platforms listed on the USGCB Web site at https://csrc.nist.gov/projects/united-states-government-configuration-baseline

3.11.3 - National Institute of Standards and Technology (NIST)

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

The Cyber Security Research and Development Act of 2002 (P.L. 107-305) tasks NIST to "develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the federal government."

CMS highly encourages business partners to review and incorporate the NIST concepts into their Medicare security program. Under the Computer Security Act of 1987 (P.L. 100-235), NIST develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. These publications present the results of NIST studies, investigations, and research on IT security issues. The publications are issued as Federal Information Processing Standards (FIPS) Publications, Special Publications (SP), NIST Interagency Reports (NISTIRs), and IT Laboratory (ITL) Bulletins.

Publications in the 800 series (SP 800-xx) present documents of general interest to the computer security community. FIPS are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (P.L. 104-106) and the Computer Security Act of 1987 (P.L. 100-235). With the passage of FISMA, there is no longer a statutory provision to allow agencies to waive mandatory FIPS. The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, any reference to a "waiver process" included in FIPS publications is no longer valid. Note, however, that not all FIPS are mandatory; consult the applicability section of each FIPS for details.

CMS does not normally require the verbatim use of NIST SPs for the configuration of Medicare systems. In cases where verbatim compliance is required, the requirements are specified in this Business Partners Systems Security Manual (BPSSM) and the MAC ARS. However, CMS highly encourages business partners to utilize NIST and other guidance documents to develop security standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

The most current NIST publications are available at: http://csrc.nist.gov/publications/index.html.

3.12 - End of Life Technology Components

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

The current HHS policy states "Operating systems, software and applications are considered end-of-life (EOL) when they are no longer supported by the vendor/provider and do not receive product updates and security patches." Standard HHS contract language requires that vendor software needs “to be within one major version of the current version”. To address both the HHS policy and the HHS contract language, and to document how the business partner has implemented the EOL control, business partners need to implement MAC ARS control SA-22, which restricts the use of unsupported information system components. For business partners, components are defined as any hardware or software used by the FISMA system.

While paying for extended support to receive security updates for all levels of severity (with a component vendor or a third-party vendor) is acceptable for meeting the HHS policy regarding EOL, business partners are expected to plan for and remove components that the vendor plans to, or currently no longer supplies security updates. If vendors can only provide updates or fixes for certain levels of security flaws (e.g. critical only), this could leave security threats and risks present in the environment and would not be acceptable for meeting the HHS policy regarding EOL.

Business partners shall demonstrate their efforts to remove these components, with documentation that can include, but is not limited to, vendor notifications, project plans and identified issues. If the components cannot be removed before security updates end because the vendor provided limited notice or because removal requires a long-term project, then the business partner shall work with CMS to implement controls to mitigate risk to an acceptable level until the component can be replaced. If the risk cannot be sufficiently reduced, the business partner shall work with CMS to open a POA&M, if necessary, prior to the end of support. In addition, business partners are required to be on either the current or the one prior major version of the component. For those situations where the business partner wants to use previous versions, and the component is supported by the vendor, then the business partner shall perform a risk analysis and document the results in the ISRA.

3.13 - Cloud Computing

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

According to NIST, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST SP 800-45). FEDRAMP has implemented security requirements for low, moderate and high risk rank systems. MACs and other business partners that are rated as high can use CSPs for non-claims processing functions with the approval of the CMS ISSO. MACs are expected to document control implementations and confirm compliance of CSP controls within their SSP. If the CSP supplied controls and services are less strict than the MAC ARS requirements, then the business partner is expected to supplement the CSP controls or implement separate controls that meet the MAC ARS. Also, other requirements that are not specifically documented in the MAC ARS or in an RMH document, such as the reporting of configuration settings are not waived with the use of a CSP; therefore, this should be carefully considered before requesting to use a CSP.

3.14 – MAC ARS Control Parameter Tailoring

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Limited tailoring of certain MAC ARS control parameters is permissible. The MAC ARS contains controls that are required to be implemented, but within certain controls, parts of the control can be tailored to meet appropriate system requirements. For controls where specific parameters are not fully documented, an acknowledgement of the parameter or setting shall be documented in

CFACTS within the control implementation section. Any tailoring is subject to review, evaluation and adjustment by CMS.

3.15 - Data Loss Prevention

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Data protection for a Business Partner's environment is critical in ensuring the privacy and integrity of their information. Business Partners must have a comprehensive Data Loss Prevention (DLP) solution in place to provide comfort that data is not being exfiltrated from their environment. The DLP solution should also provide assurance that if unauthorized data exfiltration is identified, it is blocked and the effects are mitigated. The implemented DLP solution must cover data in use (endpoints), data in transit (network), and data at rest (data storage). Several tools implemented for other MAC ARS controls, such as Malicious Code Protection (endpoints), Intrusion Detection System/Intrusion Protection System (network) and encryption (data storage) can be combined to form a DLP solution. Business partners shall maintain documentation to support the DLP solution including formally maintained policies and procedures for the tools, controls, and processes.

3.16 - Wireless Access Monitoring

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

As outlined in the MAC ARS, wireless access to a MAC network is not allowed unless explicitly approved in accordance with AC-18. MAC ARS AC-18 also states that an organization must monitor for unauthorized wireless access. Business partners must have a program in place to fulfill this requirement and have associated policies and procedures outlining how the program is operated. The implementation must be capable of identifying unauthorized wireless devices or access points that could be providing access to the network. Monitoring activities should be performed on a periodic basis as needed, but at least quarterly to confirm that unauthorized wireless access does not exist and/or is removed. If wireless access to the environment has been appropriately approved, an accurate and formally maintained listing of approved access points must be maintained to perform effective monitoring. The approved wireless access point list should be reviewed during the monitoring process to capture necessary updates.

3.17 - Malicious Code Protection

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

MAC ARS SI-3 requires that malicious code protection mechanisms be in place for an organization's information systems. If malicious code protection mechanisms are available for a system, they should be implemented and meet the requirements outlined in SI-3. If the solution in place provides malicious code protection sufficient to protect the device, however, cannot perform traditional file scanning based on the timing specified within SI-3 (e.g. AI solutions that rely on real time analysis), documentation should be maintained to demonstrate how the solution meets the security need of identifying malicious files in place of defined scanning times. In the event that an information system/platform does not have compliant malicious code protection mechanisms available for implementation, the Business Partner should put in place mitigating controls (e.g. file integrity monitoring) to assist in detecting/blocking the risk of malicious code. Documentation for these mitigating controls should be represented in formally maintained policies and procedures specific to the information systems in question.

3.18 - Whitelisting

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

MAC ARS CM-7(5) requires that defined software be documented and explicitly authorized to be allowed to be executed. This authorization of software is known as whitelisting. If the whitelisting of software is a manual process, then the process to review and update the list of authorized software programs must be completed no less often than every seventy-two (72) hours. If automated tools are used to whitelist software, then the automated tools must be updated whenever the authorized software changes or new software is authorized, and the tool must be programmed to either perform a scan of the network for unauthorized software no less often than every seventy-two (72) hours, or perform an on-demand evaluation of software every time the software is executed. In addition, management must review and formally document the list of approved software every 90 days.

3.19 – Data Encryption

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

The MAC ARS includes several controls that require data encryption; however, the language included in some of the controls appears to conflict with language in other controls. To consistently address all of the data encryption controls included in the MAC ARS, for data that is not already encrypted at rest or in transit, a risk assessment shall be completed to determine if the CIA of the data can be maintained with or without encryption. All workstations and portable media containing PII or PHI should already be encrypted. For other hardware and software maintained within the documented and approved system security boundary, where the risk assessment determines that CIA is at risk, FIPS 140-2 compliant encryption shall be implemented for data in transit and/or data at rest. If the risk assessment determines that adequate controls are in place to protect the CIA of the data while it is within the documented and approved system security boundary, then the data can be transmitted and stored in the clear. Also, when encrypting data, the method of encryption can be determined to be hardware or software as appropriate.

3.20 – Firewall Ruleset Reviews

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Firewalls are key to preventing unauthorized and unwanted network traffic from entering or exiting a network and for restricting network access as a means of enforcing least privilege access. Firewalls accomplish this using rulesets that determine which traffic is allowed to pass. The CMS TRA requires firewalls to functionally separate internal network zones.
In accordance with the latest revision of NIST Special Publication 800-41, management shall develop policies and procedures to periodically review firewall rulesets and policies (both internal and external facing) to ensure they remain in compliance with security policy. Management should use a risk-based approach for determining the frequency of the review for each firewall, but at a minimum, on a yearly basis. Areas to address in the policies and procedures include, but are not limited to:

- Validating old or out-of-date rules are prevented from processing by commenting them out or deleting them. Validating redundant rules are not active.
- Reviewing all rulesets and policies to identify that change documentation or reference information that describes the purpose are documented. Management should be able to provide business justification for each active rule.

- Testing that changes do not break or bypass existing rulesets and function as intended.
- Documenting change management processes to confirm that rule changes were reviewed, tested, and approved.
- Comparing current rulesets to secured backups to validate that no unauthorized changes have occurred.
- Verifying known insecure protocols and potentially unnecessary IP addresses are being restricted.

Firewall ruleset reviews need to be documented and evidence of review maintained. The following types of information are important to maintain with the evidence of review:

- Who reviewed the ruleset.
- When the ruleset review occurred.
- Approval of rules and tracking of rules to be removed/updated.

3.21 – Artificial Intelligence (AI)

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

There are operational and security focused tools that are changing the paradigm to increase staff efficiency and look at issues in a different way. While many of the new tools have useful new features, FISMA systems are required to follow the MAC ARS or demonstrate how the intent of the MAC ARS is being met. If an AI based tool is planned for use, then the security team needs to evaluate and document how the tool implements the MAC ARS. In addition, the following points need to be considered with implementing and maintaining an AI based solution.

- Potential issues with AI – There is often no audit trail, or supporting data, to show how the software arrived at its conclusion. Depending on the nature of a decision, supporting documentation may be needed to demonstrate how the decision was made.
- Periodic validation is required – Policies and procedures for periodic validation will need to be documented to make certain the tool is operating as intended and no security "gaps" exist. These will need to include instructions for recreating the results. If it is impossible to recreate the AI results with 100% accuracy, then tolerances need to be documented.
- Periodic assessment is required – Certain data may be used to initially seed the AI, but as conditions change, additional data may need to be added or some data may need to be removed or modified. As changes are made, associated policies and procedures may need to be updated.
- AI account management – AI tools may bring complexity with accounts needed to operate effectively. Management should treat any account, even those used for AI, with the same security requirements as their other user, service, and administrative accounts.
- AI external connections – AI tools should be evaluated to determine if the tool operation or the data being analyzed is being sent outside of the organization-controlled network (e.g. cloud repository). If so, CMS should be consulted prior to implementation.
- In the event that the AI tool being implemented cannot align exactly to part of a MAC ARS control, management should evaluate if the tool has addressed the risk of the requirement. If the tool addresses the risk but the implementation is different than what the MAC ARS identifies, this should be documented within the organizations SSP and policies. If the tool does not address the risk, then management may need to determine if additional control implementations are needed to fully address that MAC ARS control. MACs should consult with CMS if a technical limitation is encountered.

4 - Information And Information Systems Security

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

4.1 - Sensitive Information Protection Requirement

Business partners are responsible for implementing the Minimum Protection Standards (MPS) for all CMS sensitive information (digital and non-digital) and information systems categorized at the "HIGH" security level designation. The MPS establishes a uniform method for protecting data and items that require safeguarding. The MPS applies to all IT facilities, areas, or systems processing, storing, or transmitting CMS sensitive information (i.e., any information categorized as "HIGH") in any form or on any media.

Care must be taken to deny unauthorized access to areas containing sensitive systems and information during working and non-working hours. This can be accomplished by creating restricted areas, security rooms, or locked rooms. Additionally, sensitive information in any form (computer printout, photocopies, tapes, notes, etc.) must be protected during non-duty hours. This can be done through a combination of methods: secured or locked perimeter, secured area, or containerization.

4.1.1 - Restricted Area

A restricted area is a secured area whose entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas shall either meet secured area criteria or provisions shall be made to store CMS sensitive items in appropriate containers during non-working hours. The use of restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of sensitive information. All of the following procedures must be implemented to qualify as a restricted area.

Restricted areas shall be indicated by prominently posted signs and separated from non-restricted areas by physical barriers that control access. The number of entrances should be kept to a minimum and each entrance shall have controlled access (e.g., electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance should be controlled by a responsible employee positioned at the entrance to enforce the restriction of access to authorized personnel accompanied by one or more officials.

When unescorted, a restricted area register shall be maintained at a designated entrance to the restricted area and all visitors (persons not assigned to the area) entering the area shall be directed to the designated entrance. Visitors entering the area shall enter (in ink) in the register: their name, signature, assigned work area, escort, purpose of entry, and time and date of entry.

The entry control monitor shall verify the identity of visitors by comparing the name and signature entered in the register with the name and signature of some type of photo identification card, such as a driver's license. When leaving the area, the entry control monitor or escort shall enter the visitor's time of departure. Each restricted area register shall be closed out at the end of each month and reviewed by the area supervisor/manager.

To facilitate the entry of employees who have a frequent and continuing need to enter a restricted area, but are not assigned to the area, an authorized access list (AAL) can be maintained. Each month a new AAL shall be posted and vendors shall be required to sign the register. If there is any doubt on the identity of the individual prior to permitting entry, their identity shall be verified prior to permitting entry.

4.1.2 - Security Room

A security room is a room that has been constructed to resist forced entry. The primary purpose of a security room is to store protectable material. The entire room shall be enclosed by slab-to-slab walls constructed of approved materials (e.g., masonry brick, dry wall, etc.) and supplemented by periodic inspection. All doors for entering the security room shall be locked with locking systems meeting the requirements set forth below (section 4.2.5, Locking Systems). Entry is limited to specifically authorized personnel.

Door hinge pins shall be non-removable or installed on the inside of the room. Any glass in doors or walls shall be security glass (a minimum of two layers of 1/8 inch plate glass with .060 inch [1/32] vinyl interlayer, nominal thickness shall be 5/16 inch). Plastic glazing material is not acceptable. Vents and louvers shall be protected by an Underwriters' Laboratory (UL)-approved electronic Intrusion Detection System (IDS) that annunciates at a protection console, UL-approved central station, or local police station; and the IDS shall be given top priority for guard/police response during any alarm situation.

Whenever cleaning and/or maintenance are performed, and sensitive systems and/or information may be accessible, the cleaning and/or maintenance shall be done in the presence of an authorized employee.

4.1.3 - Secured Area (Secured Interior/Secured Perimeter)

Secured areas are interior areas or exterior perimeters which have been designed to prevent undetected entry by unauthorized persons during working and non-working hours. Personnel may not reside in computer rooms and/or areas containing sensitive information unless that individual is authorized to access that sensitive information. To qualify as a secured area, the area shall meet the following minimum standards:

- Enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection or other approved protection methods, or any lesser-type partition supplemented by UL-approved electronic IDS and fire detection systems.

- Unless electronic IDS devices are used, all doors entering the space shall be locked and strict key or combination control should be exercised.

- In the case of a fence/gate, the fence shall have IDS devices or be continually guarded, and the gate shall be either guarded or locked with intrusion alarms.

- The space shall be cleaned during working hours in the presence of a regularly assigned employee.

4.1.4 - Container

The term container includes all file cabinets (both vertical and lateral), safes, supply cabinets, open and closed shelving, desk and credenza drawers, carts, or any other piece of office equipment designed for the storage of files, documents, papers, or equipment. Some of these containers are designed for storage only and do not provide any protection value (e.g., open shelving). For purposes of providing protection, containers can be grouped into three general categories: locked containers, security containers, and safes or vaults.

4.1.4.1 - Locked Container

A locked container is a commercially available or prefabricated metal cabinet or box with riveted or welded seams, or metal desks with lockable drawers. The lock mechanism may be either a built-in key, or a hasp and lock. A hasp is a hinged metal fastening attached to the cabinet, drawer, etc. that is held in place by a pin or padlock.

4.1.4.2 - Security Container

Security containers are metal containers that are lockable and have a tested resistance to penetration. To maintain the integrity of the security container, key locks should have only two keys and strict control of the keys is mandatory. If combinations are used, they shall be given only to those individuals who have a need to access the container. Security containers include the following:

- Metal lateral key lock files
- Metal lateral files equipped with lock bars on both sides and secured with security padlocks
- Metal pull drawer cabinets with center or off-center lock bars secured by security padlocks
- Key lock “Mini Safes” properly mounted with appropriate key control

If the central core of a security container lock is replaced with a non-security lock core, then the container no longer qualifies as a security container.

4.1.4.3 - Safe/Vault

A safe/vault is not required for storage of CMS sensitive information. However, if used, they shall meet the following requirements:

- A safe is a GSA-approved container of Class I, IV, or V, or UL listings of TRTL-30 or TRTL-60.
- A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings that uses UL-approved vault doors and meets GSA specifications.

4.1.5 - Locking System

The lock is the most accepted and widely used security device for protecting installations and activities, personnel data, sensitive data, classified material and government and personal property. All containers, rooms, buildings, and facilities containing vulnerable or sensitive items shall be locked when not in actual use. However, regardless of their quality or cost, locks should be considered as delay devices only and not complete deterrents. Therefore, locking system must be planned and used in conjunction with other security measures.

Minimum requirements for locking systems for secured areas and security rooms are high-security pin-tumbler cylinder locks that meet the following requirements:

- Key-operated mortised or rim-mounted deadbolt lock
- Have a deadbolt throw of one inch or longer
- Double-cylinder design; cylinders have five or more pin tumblers
- Contains hardened inserts or inserts made of steel if bolt is visible when locked
- Both the key and lock shall be "off-master"

Convenience-type locking devices such as card keys, sequenced button-activated locks used in conjunction with electric strikes, etc., are authorized for use only during working hours. Keys to secured areas not in the personal custody of an authorized employee and any combinations shall be stored in a security container. The number of keys or persons with knowledge of the combination to a secured area shall be kept to a minimum.

4.1.6 - Physical Intrusion Detection System (IDS)

Physical IDSs are designed to detect attempted breaches of perimeter areas. Physical IDS devices can be used in conjunction with other measures to provide forced entry protection for non-working hour security. Additionally, alarms for individual and document safety (fire), and other physical hazards (water pipe breaks) are recommended. Alarms shall annunciate at an on-site protection console, a central station, or local police station. Physical IDS devices include, but are not limited to: door and window contacts, magnetic switches, motion detectors, and sound detectors, that are designed to set off an alarm at a given location when the sensor is disturbed.

4.1.7 - Minimum Protection Alternatives

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

The objective of the MPS is to prevent unauthorized access to CMS sensitive information. MPS requires two barriers to accessing sensitive information under normal security. The reason for the two barriers is to provide an additional layer of protection to deter, delay, or detect surreptitious entry. Because local factors may require additional security measures, management shall analyze local circumstances to determine space, container, and other security needs at individual facilities.

Table 4.1 shall be used to determine the minimum protection alternatives required to protect CMS sensitive information. Note that any of the three alternative protection standards is acceptable whenever all of the applicable perimeter, interior area, and/or container standards are met. The protection alternative methods are not listed in any order of preference or security significance.

Table 4.1. Protection Alternative Chart

	Perimeter Type	Interior Area Type	Container Type
Alternative #1	Secured		Locked
Alternative #2	Locked	Secured	
Alternative #3	Locked		Security

4.2 - Encryption Requirements for Data Leaving Data Centers

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

CMS, as a trusted custodian of individual health care data, must protect its most valuable assets—its information and its information systems. Consequently, CMS believes that putting the government's credibility at risk is not acceptable.

No data that includes personally identifiable information (PII) shall be transported from a CMS data center (including business partner data centers and subcontractor data centers) unless it has been encrypted in accordance with CMS standards. The only exception to this requirement is for hardcopy records that are transported to and from an off-site location and between off-site locations. To qualify for this exception, the controls listed below (additional information is available from CMS) shall be used.

To prepare the records for shipment:

- The records shall be stored in boxes.
- Each box shall be uniquely identified.
- Boxes shall be secured for shipment.
- Secured boxes shall be loaded into the shipping container or vehicle.
- Total items in each shipment shall be noted and the Bill of Lading signed.
- At time of pickup, the shipping company representative shall verify and sign the Bill of Lading.
- A copy of the identification records shall accompany each shipment.
- The shipping container or vehicle shall be locked and sealed with the seal number noted on the Bill of Lading.
- A copy of the completed Bill of Lading shall be kept by the contractor.

Upon receipt of the shipment at the storage facility:

- A storage facility representative shall verify the seal number and that it is unbroken.
- Compare the contents of the shipment against the Bill of Lading and the boxes against the copy of the identification record.
- If any discrepancies are found, the discrepancy shall be immediately resolved.
- After verification that all boxes shipped were received, information from the Bill of Lading shall be sent to the shipper where it shall be verified.
- Within 24 hours, all boxes on each shipment shall be scanned into the storage facility's tracking system and inserted into the storage racks.

5 – Secure Use of the Internet

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

With prior written approval of their sponsoring CMS Business Owner, business partners may use the Internet for transmission of and/or receipt of health care transactions. Each request for using the Internet to conduct CMS business functions will be considered individually and approval is not automatic. However, any approval shall require that business partners meet CMS architectural, security, data interchange, and privacy requirements for Internet-facing infrastructure. Further, an independent (third-party) assessment of security controls of the new functionality prior to its release into production is required and the assessment must include penetration testing. The assessment must be conducted to validate compliance with the following specific architectural, security, data interchange, and privacy requirements, as well as the MAC ARS. The existing requirement for an annual penetration test of the contractor network shall include any approved Internet infrastructure within the FISMA boundary. Compliance with existing MAC ARS requirements to conduct vulnerability scans and penetration testing is still mandatory.

Briefly, architectural, security, data interchange and privacy requirements include the following:

1. Architecture:

   - Explicit compliance with CMS system lifecycle standards, particularly the CMS Technical Reference Architecture (TRA), as currently released, and all its appendices.
   - Utilization of resources to leverage existing technology and solutions such as platform and software developed by contractors and in compliance with CMS standards to meet the same or similar business requirements. The technology and solutions would also have to align with requirements for the Medicare Administrative Contractors, Enterprise Data Centers, and Standard Front-End initiatives.

2. Security:

   - Full compliance with the CMS Target Life Cycle Framework (Checkpoints, Deliverables, and Activities including Security Authorization) when introducing the new functionality.
   - Satisfactory systems test and evaluation of the Internet application to include evaluation of all applicable controls in the MAC ARS.
   - Compliance with DHHS and CMS standard configuration settings.
   - Compliance with the NIST SP 800-41 *Rev. 1*, Guidelines on Firewalls and Firewall Policy; NIST SP 800-44 *Version 2*, Guidelines on Securing Public Web Servers; NIST SP 800-94 Rev. 1, Guide to Intrusion Detection and Prevention Systems (IDPS) NIST 800-111, Guide to Storage Encryption Technologies for End User Devices; NIST SP 800-113, Guide to SSL VPNs; NIST SP 800-114 Rev. 1, User's Guide to Securing External Devices for Telework and Remote Access; NIST SP 800-115, Technical Guide to Information Security Testing and Assessment; NIST SP 800-119, Guidelines for the Secure Development of IPv6; and NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing.
   - Security Authorization dependent on compliance with security control requirements and completion of documentation such as the ISRA, the security plan for the infrastructure, platform, and applications supporting the Internet functionality, and a CP for the supporting platform and application. The ISRA must address e-authentication requirements and controls for electronic transactions, or refer to a separate document if one exists. All security documentation must be developed to the CMS methodologies and procedures provided at:

http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

3. Privacy: Update the Privacy Impact Assessment (PIA) as set forth in Section 208 of the E-Government Act.

4. Data Interchange:

   - Utilization of HIPAA compliance standards for applicable transactions (i.e., claims, remittances and inquiry/response for eligibility and claim status) to be enabled by the new functionality.
   - Enabling both batch file transfer and interactive screen presentation for the HIPAA transactions.
   - 508 compliance for interactive screen presentation.
   - All Internet and non-Internet data exchange modes (i.e. Interactive Voice Recognition, Direct Data Entry, and Computer to Computer) shall return consistent data.
   - Compliance with Trading Partner authentication requirements including submitter/provider relationship for the HIPAA transactions.

Application requirements include but are not limited to the following:

1. A proof of concept/concept of operation paper describing the new application and functionality.
2. Information that the Internet service shall be extended only to entities or providers enrolled in the jurisdiction of the proposing business partner.
3. An attestation that the applicant has had a similar private-side application that has been in production for more than one year. The attestation shall describe the experience of the private-side application and how it relates to the Internet proposal.

Other application requirements may be imposed by the sponsoring CMS business component.

Additionally, business partners may also use the Internet for: 1) utilizing the IRS Filing Information Returns Electronically (FIRE) system for Form 1099 submissions, and 2) utilizing e-mail to transmit sensitive information via encrypted attachments in accordance with all applicable MAC ARS controls. An application for these uses is not required. If not already in place, contractors must install firewalls, filtering technology to screen incoming e-mail for high risk transmissions such as executables, up to date virus protection software, and intrusion detection software to utilize the Internet for these purposes.

References

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

In addition to this manual, the following documents may be referenced during the IT systems contingency planning process:

- CMS Information Security Library - https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library

- NIST Special Publication 800-34 Rev. 1, Contingency Planning Guide for Information Technology Systems, May 2010.

https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, Chapter 11.
  http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

- Federal Information System Controls Audit Manual (FISCAM), Exposure Draft, GAO-08-1029G, Section 3.5.
  https://www.gao.gov/products/gao-09-232g

- OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised,
  https://www.whitehouse.gov/omb/information-for-agencies/circulars/

- Office of Management & Budget, Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, 8 February 1996.
  http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

Appendix A:
Medicare Information Technology (IT) Systems Contingency Planning

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Table of Contents

1 Introduction

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

CMS business partners are required by the MAC ARS Contingency Planning family to develop and maintain a ITSCP. Business partners are expected to develop and test contingency plans that address key recovery scenarios that could occur as the result of a disastrous situation. While a contingency plan cannot address all possible scenarios, the plan should be structured to be useful in a variety of situations. When developing an ITSCP, the business partners are required to address all of the MAC ARS controls. The ITSCP needs to be developed in accordance with the CMS RMH Chapter 6 Contingency Planning document. In addition, NIST Special Publication 800-34 rev 1, Contingency Planning Guide for Federal Information Systems, should be reviewed. NIST identifies different components and plan types that should be documented and be incorporated in a robust ITSCP.

The purpose of this appendix is to supplement the CMS RMH manual and NIST publication and to provide information to aid the business partner in planning for and responding to an emergency or system disruption, and to recover from that emergency or disruption. It is to be used by the CMS Medicare business partner management, IT systems management and staff, and system security persons charged with preparing for continuing the operation of Medicare systems and developing an ITSCP, or updating an existing plan. In addition, the business partner's SSP and ISRA should be used as a checkpoint to determine if appropriate contingencies have been addressed in the ITSCP. Also, the ITSCP should be coordinated with the Incident Response activities to address the restoration and recovery activities associated with an incident.

It can be noted that an ITSCP can be out of date shortly after it is created and updated. Automated tools exist to facilitate the development and maintenance of a plan. These tools can significantly help keep a plan current, but they may not address all of the areas required and they may not format the data in a manner that is consistent with CMS requirements. In these situations, the business partner will need to supplement the tools with additional information and cross references to ensure that all required information is documented.

2 Scope

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

The business partner ITSCPs address organizations and sites where Medicare data is processed, including claims processing locations, data centers, and other processing or printing sites.

3 Definition of an Acceptable ITSCP

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

An ITSCP is a document that describes how to deal with an emergency or system disruption. These situations could be caused by, but not be limited to, a power outage, hardware failure, fire, or terrorist activity. An ITSCP is developed and maintained to ensure quick, appropriate, effective, and efficient response in those situations for which a foreseen risk cannot be mitigated or avoided.

Before developing an ITSCP, it is advisable to have or create a contingency policy. The contingency policy is a high level statement relative to what the management wants to do to address a contingency and to recover from the emergency or system disruption.

The ITSCP shall be developed under the guidance of IT management and systems security persons and all organizational components shall be actively involved in providing information for developing the plan, for making plan related decisions, and for providing support to plan testing.

It can be a subjective argument relative to what constitutes an acceptable ITSCP. In this document, the description of an acceptable ITSCP is based on the results of the research, analysis and review of various documents from Government and industry, and the review of existing business partner ITSCPs and test reports.

The following summary statements define what constitutes an acceptable ITSCP. This is not an all- inclusive list and the topics are not in any order of importance or priority.

1. Considers the protection of human life as the paramount guiding principle.

2. The backup, recovery, and restoration of critical business functions, protecting equipment and data, and preserving the business reputation for providing high-quality service.

3. Is logical, reasonable, understandable, user friendly, and can be implemented under adverse circumstances.

4. Considers risk assessment results.

5. Addresses possible and probable emergencies or system disruptions that would require the implementation of the ITSCP.

6. Can be sufficiently tested on an established regular basis within recommended recovery periods at reasonable cost.

7. Contains information that is needed and useful during an emergency or system disruption.

8. Can, when implemented, produce a response and recovery, such that critical business functions are continued.

9. Specifies the persons necessary to implement the plan, and clearly defines their responsibilities.

10. Clearly defines the resources necessary to implement the plan.

11. Reflects what can be done – is not a wish list.

12. Assumes people shall use sound judgment, but will need clearly stated guidance, since they will be functioning in a non-normal environment, under possibly severe conditions and pressure.

13. Addresses backup and alternate sites.

14. Addresses the use of manual operations, where appropriate and necessary.

15. Contains definitive "Call Lists" to use for contacting the appropriate persons in the proper sequence. These lists would include vendor points of contact.

An acceptable ITSCP should be concise. It should not contain any more information than is necessary to plan for and implement contingency actions. The users should not get bogged down in detail as they read the plan to determine what to do, when to do it, what is needed to do it, and who should do it. The ITSCP should serve as a "user's manual" and be easy to understand and use.

Because an ITSCP is designed to be used in a stressful situation, it shall be written with that as a foremost thought in mind. The prime objective is to maximize the continuity of critical operations.

Reviewing an ITSCP and testing it will help determine whether it remains an acceptable plan. The review and testing shall not focus solely on content, but shall also focus on ease of use.

Careful thought should be given to the organization of the ITSCP. The organization should be logical in terms of what will the user want to know or do first. If the first thing that should happen in an emergency is that a call list shall be used to notify persons, then that call list, or a pointer to it, should be placed very near the front of the ITSCP. Not every informational item to be utilized during a contingency event will be in the ITSCP document. For example, the plan may point to an attachment or to a separate procedures manual. It is imperative to assure that any information provided in a separate procedures manual is readily available, easily obtainable and searchable.

Contingency planning can provide a cost-effective way to ensure that critical IT capabilities can be recovered quickly after an emergency. IT systems contingency planning shall embrace a coordinated contingency policy of what will be done to fully recover and reconstitute all operations.

4 IT Systems Contingency Planning

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

The goal of IT systems contingency planning is to continue accomplishing critical IT systems operations in an emergency or system disruption and to accomplish a rapid and smooth recovery process.

4.1 Contingency Planning

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Contingency planning is preparing for actions in the event of an emergency situation, and giving some thought and planning to what your organization will do to respond and recover. The IT systems contingency planning process shall address all the actions and resources needed to ensure continuity of operation of critical IT systems and the means of implementing the needed resources. IT management and staff shall be trained to handle emergency or system disruption situations in data centers and other areas where data processing systems are located. Contingency planning includes such training.

It is advisable to establish an IT systems contingency planning team. This team would be responsible for defining critical IT systems, including applications software, data, processing and communications capabilities, and other supporting resources. These would be the key people in the implementation of the plan.

4.2 Coordination with Other Business Partners

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

If a business partner's data center or other data processing environment is linked to other business partners for the transmission of Medicare data, then the contingency planning shall address those links relative to receiving input, exchanging files, and distributing output. If alternate/backup IT systems capabilities are to be utilized, then their functions and data transmission links shall be considered in the planning.

Coordination with other business partners is essential to completing the IT systems contingency planning process.

5 IT Systems Contingency Plan

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

The following required content, in conjunction with the format contained in the CMS RMH may be used in developing an IT Systems CP.

The following checklist provides a means for determining if a CP contains the appropriate information that can readily be used in handling an emergency or system disruption. This list is not all-inclusive, but rather should serve as a thought stimulus for evaluating CPs.

This checklist uses the same outline as the suggested CP format.

1. Introduction
   Does the CP contain:

   - Background
     Is a history of the plan provided? Are the physical environment and the systems discussed?

   - Purpose/Objective
     What does the plan address? Why was it written? What does it aim to accomplish?

   - Management Commitment Statement
     Has the CP been approved by management and the SSO? Once the CP is created, reviewed, and ready for distribution, it shall be approved by site, operations and information systems management, and the SSO.

   - Scope

Are the boundaries of the plan indicated? What organizations are involved, not involved?

- Organizations
- Systems
- Boundaries
- External Interfaces

- IT Capabilities and Resources

  Is the focus of the plan on IT systems, capabilities, and resources?

- CP Policy
  - Priorities
    - Are the CP steps ranked according to priority?
  - Continuous Operation
    - Are there functions, processes, or systems that are required to continue without interruption?
  - Recovery after Short Interruption
    - Which functions, processes, or systems can be interrupted for a short time?
  - Recovery Times?
    - Are the recover times stated?
    - What are the minimum recovery times?
  - Standalone Units
    - Does a CP exist for any standalone workstation? A key part of a CP shall address any standalone workstations that are part of the critical operations environment. It shall state where backup software and support data for these workstations is stored.
    - Is the plan reviewed and approved by other key affected persons?

2. Assumptions

   Are all the important assumptions listed? Have the assumptions been carefully reviewed by the appropriate persons to ensure their validity?

3. Authority/References
   - Who or what document is authorizing the creation of the CP?
   - What are the key references that apply to the plan?

4. Definition of what the CP Addresses
   - Organizations

     To which organizations does the CP apply?
   - Systems

     Is there a general description of systems and/or processes?
   - Boundaries

     Are the system boundaries clearly defined?

- External Interfaces

Are external interfaces clearly defined?

5. Three phases defined
   Does the plan address three phases of emergency or system disruption?

   - Respond
     - Is this phase adequately described so that it is understood what activities occur therein?
     - Are people, and their safety, considered?
     - Is damage/impact assessment considered?
     - Are the alerting and initial impact assessment procedures fully explained as well as arrangements for continual review of their use and effectiveness?

   - Recover
     - Is this phase adequately described so that it is understood what activities occur during this phase?
     - Are effective recovery strategies in place for hardware, software and data?
     - Are hardware configuration and operating system requirements considered?
     - Have interdependencies between internal and/or external systems considered?

   - Restore/Reconstitute
     - Is this phase adequately described so that it is understood what activities occur during this phase?
     - Has validation of data been documented?
     - Has a clear path for validating system functionality and operational capabilities been implemented?

6. Roles/Responsibilities Defined

   - Has the necessary CP implementation organization been defined and the responsibilities of all those involved clearly stated with no 'gray areas'?

   - Will all who have a task to perform be aware of what is expected of them?

   - Does the CP assign responsibilities for recovery? The responsibilities of key management and staff persons shall be carefully described in the CP, so that there is no question relative to the duties of these people during an emergency.

7. Definition of Critical Functions

   - Does the CP address critical systems and processes?

   - Have emergency processing priorities been established and approved by management?

   - Does the CP specify critical data? The CP shall specify the critical data needed to continue critical business functions and how frequently the data is backed up.

   - Has a list of critical operations, data, and applications been created? In preparing the

CP, a list of current critical operations, data and applications shall be documented and approved by management. This list shall contain the items needed to continue the minimum critical business elements and functions until operations could be returned to a normal mode.

8. Alternate Capabilities and Backup

- Have arrangements been made for alternate data processing and telecommunications facilities? Part of contingency planning includes the completion of arrangements for alternate data processing facilities and capabilities, and for alternate telecommunications capabilities necessary to re-establish critical interfaces.

- Does the CP address issues relative to pre-planned alternate locations? The CP shall address any potential issues relative to pre-planned alternate locations. These include:
    - insurance
    - equipment replacement
    - phones
    - utilities
    - security

- Does contingency backup planning exist? Planning for appropriate backup of data and processing capabilities shall include:
    - prioritizing operations
    - identifying key personnel and how to reach them
    - listing backup systems and where they are located
    - stocking critical forms, blank check stock, and supplies off-site
    - developing reliable sources for replacing equipment on an emergency basis

- Is there an alternate information processing site; if so, is there a contract or interagency agreement in place?

- Are the levels of equipment, materials and manpower sufficient to deal with the anticipated emergency? If not, have back-up resources been identified and, where necessary, have agreements for obtaining their use been established?

- Have temporary data storage sites and location of stored backups been identified?

- Is the frequency of file backup documented?

- Have the arrangements been made for ensuring continuing communications capabilities?

- Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?

- Are system, application, and other key documentation maintained at the off-site location?

- Are the backup storage and alternate sites geographically removed from the primary site and physically protected?

- Do data and program backup procedures exist? In order to be prepared for an emergency, it is advisable to provide backups of critical data and software programs. These are stored at off-site locations sufficiently distant from the primary site so as not to be affected by the same emergency that would affect the primary site.

- Is the CP stored off-site at alternate/backup locations? Copies of the CP shall be stored at several off-site locations, including key personnel homes, so that at least one copy is readily available in time of emergency. Copies of the CP that are stored in a private home shall be protected from inadvertent access.

9. Required Resources

- Are the following resources for supporting critical operations defined and available for an emergency?
    - Hardware
    - Software
    - Communications
    - Data
    - Documents
    - Facilities
    - People
    - Supplies
    - Basic essentials (water, food, shelter, transportation, etc.)

- Does the CP provide for backup personnel? As the CP is implemented, it is necessary to have additional people available to support recovery operations. The CP shall specify who these people are and when they would normally be called into action.

10. Training

- Are management and staff trained to respond to emergencies? Security training shall include modules for management and staff relative to their roles for handling emergency situations.

11. Testing the CP

- Is there a section in the CP that addresses testing of the plan?
- Testing of the CP shall address the following topics:
    - Test Philosophy
    - Test Plans
    - Boundaries
    - Live vs. Walkthrough vs. End-to-End Testing
    - Test Reports
    - Responsibilities

12. CP Maintenance

- Schedule
    - Is the CP annually reviewed and tested within every 365 days? The CP shall be reviewed and tested under conditions as close to an emergency as can be reasonably and economically simulated.
    - Is there a provision for updating the CP within every 365 days?
    - Is the CP revised after testing, depending on test results? Are lessons learned

documented and incorporated into the revise CP?

13. Relationships/Interfaces

- Does the CP identify critical interfaces? Interfaces required to continue critical business functions should be identified. Refer to the System Security Plans.

- Which outside (vendors, providers, banks, utilities, services, CMS) interfaces must be considered?

- Is the plan compatible with plans of interacting organizations and systems?

- What internal interfaces must be considered?

- Which corporate interfaces must be considered?

- Are there special interfaces with corporate systems that must be addressed in the CP?

14. Attachments

Does the CP contain appropriate attachments, as listed below?

A. Actions for Each Phase

Are the actions to be taken in each phase (respond, recover, restore) of the contingency clearly described and related to organizations and/or people?

B. Procedures

- Are there detailed instructions for:
  - responding to emergencies?
  - recovering operations?
  - restoring operations?

- Do contingency backup agreements exist? Agreements with organizations or companies which will provide service, equipment, personnel, or facilities during an emergency shall be in place.

- Are there procedures for addressing the situation where the processing site is intact, but people can’t get to it because of a natural disaster? Can the business be operated remotely?

- Is there an implementation plan for working from home?

C. Call Trees

Are there call lists with names, addresses, and phone numbers with priority order relative to whom to call first?

D. Hardware Inventory

Are there lists of all the hardware covered by the CP?

E. Software Inventory

Are there lists of all the software covered by the CP?

F. System Descriptions

Are all the systems covered by the CP defined, including appropriate diagrams?

G. Alternate/Backup Site Information

Is there sufficient detail to completely describe the alternate and/or backup sites, including addresses, phone numbers, contacts, resources available at the sites, and, resources needed to be brought to the site?

H. Assets/Resources

Are there lists of all the needed resources for responding, recovery, and restoring operations?

I. Risk Assessment Summary

Has there been a realistic assessment of the nature and size of the possible threat and of the resources most at risk?

J. Agreements/Memo of Understanding

Are there agreements in place relative to the use of alternate/backup sites, special resources, outside suppliers, extra people, alternate communications, etc?

K. Manual Operations

Are manual operating procedures in place so that certain functions can continue manually if automated support is not available soon enough?

Manual processing procedures shall exist in the backup phase until automated capabilities can take over the information processing. Provisions shall be made to provide this manual capability.

L. Supplies/Materials/Equipment

Is there information that describes how and where to obtain needed supplies, materials, and equipment?

M. Floor Plans

Are the necessary floor plans available?

N. Maps

Are the necessary area and street maps available?

O. The CP shall provide for off-site storage:

- Backup software
- Data
- Appropriate documents (emergency telephone lists, memos of understanding, etc.)
- Copies of the CP
- Administrative supplies (forms, blank check stock, etc.)

6 Testing

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

CMS requires testing of the CP annually under conditions that simulate an emergency or a disaster. A CP shall also be tested after a substantive system change that necessitates a revision to the CP.

CMS requires that the critical IT systems shall be tested within every 365 days and the CP updated to accommodate any changes, including updated versions of software or critical data. Critical systems are those whose failure to function, for even a short time, could have a severe impact, or have a high potential for fraud, waste, or abuse.

6.1 CMS Virtual Data Centers (VDC)

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Some contractors with which CMS has direct contracts do not have their own data centers. If a business partner does not have its own data center, then it is the responsibility of the business partner to inform the subcontractor that operates the data center that they shall have a CP that addresses the requirements outlined in the Appendix.

6.2 Multiple Contractors

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

The VDCs usually serve multiple contractors. Existing shared processing environments allow for multiple contractors to process claims at a data center. There are several data centers processing Part A and Part B claims for multiple Medicare contractors.

It is important to test a CP with a data center that serves multiple contractors. This provides an opportunity for the business partner to validate that they can recover the connection with the VDCs to process claims.

6.3 Test Types

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

CP test guidance suggests four types of testing:

- Walkthrough/Tabletop Test
- Checklists
- Simulation/modeling
- Live/Comprehensive Exercises

These are defined below:

- **Walkthrough/Tabletop Test**: A walkthrough test is accomplished by going through a set of steps to accomplish a particular task or action initiated because of a contingency event. The precursor to a walkthrough test is that the steps are documented so that they can be logically followed. A "test team" might sit around a table and talk through each step and then walk through" the various steps, and then discuss expected outcomes and further actions to be taken. They may use a checklist to ensure that all features of a step are addressed or that all resources necessary to accomplish the task or action are considered. A walkthrough test does not involve accomplishing the actions being tested in real time or using the live environment. A walkthrough test could be accomplished by using a group of test people to act out what might happen if a real contingency event occurred. They might go to the alternate site, but they would not actually start all hardware, software, and communication operations in order to assume the function of the primary site.

  For those applications that are both hosted at CMS and not participating in a broader recovery test to a CMS-approved recovery site during their annual test cycle, a tabletop test is required. A tabletop test is discussion-based only, and does not involve deploying equipment or other resources. The discussion during the test can be based on a single scenario or multiple scenarios. By simulating an emergency in an informal, stress- free environment, this test method allows for the free exchange of ideas and provides participants an opportunity to practice the steps to be followed in an actual event and to identify areas in the CP for enhancement.

  A successful tabletop test steps participants through real-life scenarios; captures its results in a formal report; and incorporates the "lessons learned" into subsequent versions of the CP and the tabletop test plan.

- **Checklists**: Checklists are used to clearly present a step-by-step logical sequence so systems and sub-systems may be recovered in a logical manner. Checklists are intended to provide a direct, simple coordinated listing of events that ensure that all necessary steps are executed during the recovery process.

- **Simulation/Modeling**: Modeling involves creating a computer model of the process to be tested. This allows easy testing of many variables without physically having to make changes. For example, you can vary the number of servers that go down during a disaster or the number of people that can get to an alternate site following a disaster.

  Simulation involves taking physical actions, but not necessarily to the full extent of what might actually happen during an emergency. For example, instead of actually moving everyone to an alternate site to continue operations, a small team may undertake a set of realistic preparatory actions at the prime site, and another team does the same at the alternate site. Thus, many steps could be simulated by the two teams and worthwhile results evaluated.

- **Live/Comprehensive Exercises**: This is the most complete and expensive test to accomplish. It involves completing the physical steps that would actually be taken if an emergency occurred. People and materials would be moved to an alternate site for the test, and servers would actually be shut down to reduce capability. Power would be shut off, and live conditions would be tested. A live test uses actual environments, people, and components to accomplish the test in real time. It is the real thing, nothing artificial, or made up, is substituted. If the test is to see if an alternate site capability can be implemented, then in a live test, the hardware, software, data, communications, and people at the alternate site would be set into action and begin functioning as the primary site to support operations.

End-to-end refers to the scope of the testing (partial testing is less than end-to-end). When conducting end-to-end testing, items to consider include:

- End-to-end testing can be completed as part of walkthrough or live test.

- Not testing end-to-end means that some links, processes, or subsystems are missed.

- What is the risk in not conducting end-to-end testing?

- Live end-to-end testing can be very expensive!

Considering risks and cost, management shall make a decision as to what type and scope of testing is appropriate.

6.3.1 Live vs. Walkthrough

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

- High-level testing can take the form of a walkthrough test.

- A walkthrough can be part of the overall testing process, but not the whole process.

- Lower-level testing can include a walkthrough, if live testing is not an option.
    - Live testing shall be the first choice.
    - Fall back to a simulation/model if live testing is not an option.
      Cost, time, and interruption of normal operations are major considerations in doing a live test.
    - A walkthrough test should be the last resort.

- Consider what a walkthrough test would miss.

- Consider the risks of missing that part of the test.

- Remember that there is risk in not doing a live test—is the risk acceptable?
    - Consider the criticality of functions, processes, and systems.
      If critical to continuing essential business operations, then these are strong candidates for live testing.

- Testing interfaces.
  It is important to test the critical interfaces with internal and external systems. It is difficult to test interfaces using a “walkthrough” method. Simulation or “live” testing is preferred.

- Cost and complexity.
  The decision as to how to test critical functions, processes, and systems must result from

careful consideration of complexity and cost. A complete “live” test of all elements of an operation may prove to be extremely costly, in terms of both dollars and time. If that cost outweighs the “cost” of the risk of not doing live testing, then “live” testing should probably be ruled out.

6.3.2 End-to-End

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

This kind of testing aims to ensure that all software and hardware components associated with a function, process, or system are tested from the front end through to the back end (input through process through output). As with live testing, end-to-end testing can be expensive.

- End-to-end testing shall only be considered for critical functions, processes, or systems.

- End-to-end testing provides the best assurance that there are no problems.

- If the overall process to be tested can be sub-divided into critical and non-critical components, then only the critical components need be considered for end-to-end testing.

- Examples of types of end-to-end tests:
    - Claims receipt through to check generation
    - Query of a database through to the response
    - Medicare Secondary Payer (MSP) check request through to check issue and back to MSP

- The decision on how to test critical functions, processes, and systems shall carefully consider complexity and cost. A complete end-to-end test of all elements of an operation may prove to be extremely costly, both in terms of dollars and time. If that cost outweighs the cost of the risk of not doing end-to-end testing, then end-to-end testing should probably be ruled out.

- Look at the criticality of functions, processes, and systems. If these are critical to continuing essential business operations, then these are strong candidates for end-to-end testing.

- If you cannot do end-to-end testing, then consider live testing of all possible connections to help ensure minimum problems.
    - Or, do simulation/modeling
    - Or, do walkthrough

Overall, end-to-end testing may combine walkthroughs, simulation/modeling, and live testing of contingencies. Walkthroughs and simulations may be used for non-critical systems, whereas critical systems shall be functionally tested under conditions that reproduce an emergency or a disaster.

It is advisable that the testing of critical systems be done end-to-end, input through output, so that no physical activity, automated process, or Medicare business partner system is left untested. Critical interfaces internal and external to the systems shall be tested.

6.4 Test Planning

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

An ITSCP test plan shall address at least the following:

- Test objectives
- Test approach
- Required equipment and resources
- Necessary personnel
- Schedules and locations
- Test procedures
- Test results
- Failed tests
- After Action Report
- Retest
- Approvals

It is advisable to establish test teams responsible for preparing and executing the ITSCP tests. Responsibilities shall be assigned to test team members, including executives, observers, and contractors.

Following testing, any corrections specified in an After Action Report shall be included in the next ITSCP test. The process shall include:

- List of items that failed the previous test
- Corrections planned
- Retest detail
- Schedule
- Review responsibilities

Ensure that the lessons learned from ITSCP testing are formally discussed among senior business partner management, operations, IT management and staff, and the SSO.

Documentation shall exist for:

- Test plans
- Test results
- After Action Report
- Retest plans
- Memos of Understanding/Formal Test Arrangements
- Lessons Learned

7 Maximum Tolerable Downtime (MTD)

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

MTD is the time it takes to recover an operation, function, process, program, file, or whatever has to be recovered as an operational entity. If claims processing operations must be recovered within 72 hours, then that is the MTD to recover. Anything over that is unacceptable.

- Recovery times may vary, depending on the criticality of the function involved.

- Times can be from a few minutes to days or weeks.

- A table/matrix can be constructed that lists the recovery times.

- There can be a separate table/matrix for each major function (e.g., claims processing, medical review, check generation).

- Recovery times shall be clearly defined and must be achievable.

8 Responsibilities

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Following is a summary of responsibilities for key groups and persons involved with developing business partner ITSCP.

8.1 Business Partner Management

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

- Defines scope and purpose of IT systems contingency planning.

- Authorizes preliminary ITSCP planning.

- Ensures that appropriate ITSCPs are developed, periodically tested, and maintained.

- Ensures that all IT operations participate in the planning and development of the ITSCP.

- Reviews the ITSCP and documented recommendations.

- Requests and/or allocates funds for plan development and approved recommendations.
- Assigns teams to accomplish development of test procedures, and for testing the ITSCP.

- Reviews test results and document an After Action Report.

- Ensures that the appropriate personnel have been delegated and notified about the responsibility for effecting backup operations, and that the backup copies of critical data are ready for use in the event of a disruption.

- Ensures that the business partner organization can demonstrate the ability to provide continuity of critical IT systems operation in the event of an emergency.

- Business partner management shall approve:
    - The ITSCP
    - Changes to the ITSCP
    - Test plans
    - Test results
    - Corrective action management processes

  - Retest plans
  - Memos of Understanding/Formal Arrangement Documents
  - After Action Report
  - Changes to storage and backup/alternate site facilities

8.2 Systems Security Officer (SSO)

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

- Documents the scope and purpose of ITSCP
- Reconciles discrepancies and conflicts in the ITSCP
- Evaluates security of backup and alternate sites
- Leads the preparation of the ITSCP
- Submits the ITSCP and recommendations to Business Partner Management
- Monitors implementation of the ITSCP and reports status to Business Partner Management
- Ensures all testing of the ITSCP is performed in accordance with CMS requirements
- Reviews test results
- Ensures that the ITSCP is updated based on test results
- Ensures lessons learned are discussed and formally documented in an After Action Report
- Obtains approval from the CMS Business Owner

9 ITSCP Changes

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

The ITSCP shall be reviewed/updated whenever one or more of the following events occurs:

- New systems or operations added.
- Upgrade or replacement of Standard System software.
- Hardware or software replacement.
- Changed back up/alternate site.
- Changed storage facilities.
- Removal of existing systems or operations.

9.1 ITSCP Attachments

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

Materials that are too extensive to be included in the body of the Medicare ITSCP shall be included as attachments. These shall be kept current and referenced in the ITSCP. All attachments shall be available to appropriate ITSCP personnel. These shall also be a part of the System Security Profile. The SSO shall ensure that the information to be attached is pertinent and current, and that updated copies are routinely incorporated, particularly into offsite copies of the ITSCP

Appendix B:
An Approach to Fraud Control

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Table of Contents

1 Introduction

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

This document develops countermeasures relating to fraudulent acts and a checklist to help Medicare contractors assess their vulnerability to fraud. Fraud and embezzlement are skyrocketing, largely because basic safeguards are neglected or lacking. Fraudulent acts are discussed in terms of the types of safeguards in place and functioning.

2 Safeguards against Employee Fraud

(Rev.11570; Issued: 08-19-22; Effective: 03-07-23; Implementation:04-03-23)

The following safeguards are specific countermeasures against fraudulent acts by employees whose functions involve Medicare program funds. These safeguards are consistent with the MAC ARS, and do not constitute wholly different or additional minimum requirements. The following countermeasures should prove especially effective against currently prevalent fraudulent activities and are discussed primarily as they relate to prevention and detection of fraud.

A. Screen New Employees

Screen new employees for positions that involve program funds directly or indirectly to address the applicant's past faithful and honest performance of duties with other employers in addition to job performance and investigation of his/her personal finances. New employees' statements concerning personal finances shall be confirmed with former employers and with banking and credit institutions. Phone calls to previous employers are essential, particularly to former supervisors who should be advised of the nature of the position. Although former employers will sometimes fail to prosecute employees associated with fraudulent activities, they seldom delude a prospective employer asking about the applicant's integrity.

Any blatant dishonesty in the application (such as claiming qualifications and experience the applicant never had) shall remove the applicant from further consideration. Check references and crosscheck them (one against the other) for consistency as well as content. Evaluate references on the basis of the contact's personal knowledge of the applicant's job-related qualifications and integrity.

Proper screening is preventive medicine at its best. Gaps in employment are flags that call for third-party verification, not just a plausible explanation by the applicant. Former employers may be able to shed light on the situation or be able to relate the reason given them about gaps by the applicant.

Circumstances relating to termination of previous employment should be clearly related by former employers. Resolve any inconsistencies or vagueness.

Ask former employers as well as the applicant, whether the employee was ever bonded, or was ever refused bonding. Sensitive screening should not result in violating an applicant's civil rights, while assuring you (and your bonding company) that prudent concern is exercised in the hiring process.

B. Bonding

Bonding is also known as fidelity insurance and comes in all configurations; the broader the coverage, the more expensive the premium. One of the most important things you can do is analyze the extent and conditions of coverage in relation to possible misappropriations of funds. Liability is invariably limited in some respects. For example, coverage often does not extend to external fraud; to losses not proven to have been caused by fraudulent acts by covered employees; to frauds committed by employees known to have perpetrated dishonest acts previously; to frauds whose circumstances are not properly investigated; or to frauds whose alleged perpetrators are not brought to trial. Inherent in the analysis of bonding is risk analysis of fraud in relation to specific components to develop a worst-case fraud scenario in terms of dollar-loss before recovery through bonding.

C. Separation of Duties

Separate duties so that no one employee can defraud the company unaided. This is the cardinal rule for fraud prevention, one that is well-understood in manual operations. It is not as well understood in its application to computer processing where a single automated system may combine functions ordinarily separated, such as transactions and adjustments. Analyze all duties, including all stages of computer programming and operations, in terms of defeating single-handed fraud as well as in terms of effectiveness and efficiency, with fraud controls taking precedence. Group review of programmer code before allowing new/upgraded systems into production is the type of duty-separation (function vs. approval) that serves both effectiveness and security.

D. Rotation of Duties

Rotate duties, particularly those involving authorization of a transaction. Separation of duties makes it difficult for an employee to defraud your organization unaided, so that embezzlement becomes a crime of collusion. As more and more embezzlement involves more than one person, it becomes necessary to ensure that the same person is not always involved in approving another's functions. An employee is less likely to initiate a fraudulent transaction if he/she is not certain that his/her accomplice will be the one to approve or process that transaction. Moreover, the knowledge that from time to time other employees will perform his/her function or work his/her cases is a powerful deterrent to any fraudulent scheme, particularly embezzlement which requires continual cover-up.

E. Manual Controls

Manual controls are differentiated from automatic controls because constant review is necessary to see that they are in place and working. Moreover, they often supplement or augment automatic controls; for example, the manual review of claims rejected in computer processing. Review all manual controls to determine the extent to which they would be effective against fraud in any operational area; too often, controls are reviewed without fraud specifically in mind. Classic manual controls are those associated with the tape/disk library, and these controls are strongly associated with restricted access and separation of duties. It does little good to separate programmer/operator duties if the programmer is allowed to sign out production tapes or master files for any reason, especially live-testing. Library controls shall require specific authorization for tape removal for specific periods for specific reasons known to, and sanctioned by, the approving authority. The most important manual controls are those over blank-check stock and the automatic check-signer. The employee in control of the check-signer shall not at the same time control the check stock, although these duties may be rotated so that the person controlling the check-signer one day may be assigned to control check stock on the following day when a third person is responsible for the check-signer. However, no one individual shall be allowed to "sign" a check he/she has issued. Rotation of duties is proper only for subsequent operations where one's own previous actions have already cleared.

F. Training

Training employees in their responsibilities relative to fraud in their operations is basic to prudent management. This extends beyond the employee's own activities. For example, Title 18, U.S. Code Section 4 requires anyone having knowledge of a

Federal crime to report it to the Federal Bureau of Investigation (FBI) or similar authority, with penalties of up to $500 fine and 3 years in jail for failure to do so. No employee should be ignorant of this responsibility. This responsibility can be explained as a simple good citizenship requirement and not spying or snitching. Discuss these things periodically in meetings, along with free give-and-take on moral issues and management's position on every aspect of fraud, including perpetration involving collusion with outsiders. Do not single out any employee or function in these discussions, instead make management's position clear regarding so-called "justification" for unauthorized "borrowing" and the fact that fraud can and will be prosecuted. Explain that there can be no permissive attitude towards dishonest acts because such an attitude is corrupting and makes it difficult for employees to remain honest. Make it known that there are controls throughout the organization to prevent and detect fraud, without being specific as to how they work. Require employees to report apparent loopholes in security that might one day (or already) be exploited for fraudulent purposes. Remind employees that ethical conduct requires their full cooperation in the event of any fraud investigation, and when interviewed they shall be called upon to explain why security gaps or suspicious activities were not reported to the SSO. No security program can be effective without the involvement and cooperation of employees, and nowhere is this truer than with fraudulent activity.

G. Notices

Notices, both periodic and situational, are effective and necessary in the prevention and control of fraud. It is not enough to formulate management policy or to conduct employee training relative to fraudulent activity. It is possible to remind employees of management's continuing concerns and to evaluate employee awareness through simple reminders or announcements of what is happening relative to fraud controls (of a general nature) and management's reliance on their cooperation and understanding of their responsibilities. Without this evidence of sustained management commitment, policy utterances tend to fade from memory or become regarded as part of a new employee's orientation and not part of the scene. This is true of minor abuses, but is also true of abuses that escalate into fraud.

H. Automatic Controls

Automatic controls to prevent or detect fraudulent activities comprise the first line of defense in computer operations. Such controls are often thought of as ensuring data integrity but more in terms of accuracy than of honesty. Evaluate automatic controls in terms of preventing payment to unauthorized persons. Test automatic controls with fraudulent (invalid) input, under strict control of courses, and with management's full cognizance and prior approval.

I. Audit Routines

Audit routines are those programs where trained auditors test for fraud using special routines to reveal computer processing that creates or diverts payments to employees or their accomplices. Wrongdoers not only have to create bogus payments, but also they have to be able to lay their hands on the checks in order to cash them. Devise audit routines to single-out payments being directed to post office boxes or to repeat addresses (where such repeats would be unreasonable), to the addresses of an employee or his family, or to a drop-off address that is not a real business but merely a place to collect mail.

3 Checklist for Medicare Fraud

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

This checklist represents questions to address in analyzing the security of Medicare fiscal operations.

1) Have Medicare operations been identified where fraud or complicity in fraud may be possible (e.g., initiation/approval of payments)?

2) Have individuals been assigned fraud-protection responsibilities in such components, including the responsibility for reporting possible fraud and vulnerability to fraud?

3) Do individual employees at all levels understand that management policy relative to fraud is dismissal and prosecution?

4) Are fiscal operations regularly audited relative to fraud vulnerability?

5) Are fraudulent acts specifically mentioned in the employee's code of ethical conduct?

6) Is employee integrity specifically addressed during the hiring process, and do background investigations elicit information that would uncover an applicant's past fraudulent activity with other employers?

7) Are operations set up in such a way as to discourage both individual and collusive fraudulent activity?

8) Are programs/systems tested by authorized individuals with “fraudulent” input?

9) Are audit trails generated that identify employees who create inputs or make adjustments/corrections that would pinpoint responsibility for any fraudulent act?

10) Is there an effective mechanism for detection/prevention of payments being

purposely misdirected to employees, relatives, or accomplices?

11) Are new or changed programs specifically reviewed for fraudulent code by those responsible for production-run approval (persons empowered to review changes but not to make changes themselves)?

12) Are controls designed to prevent fraud, especially in those operations where large sums could be embezzled quickly?

13) Are all error-conditions checked for fraud potential?

14) Are balancing operations done creatively so that an embezzler could not hide discrepancies?

15) Are the official activities of all employees, at all levels, subject to independent review by different reviewers (i.e., not always by the same evaluator)?

16) Does management insist on integrity at all levels?

17) Has management announced that employee's work activities will be reviewed (in unspecified ways) for both the fact and appearance of integrity?

18) Do tape/disk library controls in fact prevent tampering with files/programs for fraudulent purposes?

19) Are alternative fraud controls invoked during emergencies?

20) Are suspected frauds investigated promptly and properly and are they thoroughly documented?

21) Are fraud audits conducted both periodically and randomly?

22) Are random samples taken of claims/bill inputs and checked back to their sources?

23) Does the Personnel Department check the applicant's background, employment record, references, and possible criminal record before hiring?

24) Are badges, identification cards/numbers, and passwords promptly issued and rescinded?

25) Is off-hours work supervised, monitored, or otherwise effectively controlled?

26) Are all employees required to take their vacations and are their replacements required to check over the vacationers' past activities?

27) Are the credentials of outsiders, such as consultants and auditors, checked out?

28) Is temporary help bonded, hired from reputable agencies, and their activities restricted to the tasks to be performed? (Same principle applies to employees temporarily borrowed from non-Medicare components.)

29) Are written procedures controlled and restricted to employees currently assigned the relevant duties?

30) Are special fraud controls specified for backup operations?

31) Are incoming checks, including returned checks, handled by two or more individuals in the mailroom and are such teams switched around so that the same people are not always working together?

32) Are blank checks and automatic check-signing equipment strictly controlled with a tamper-proof numbering mechanism?

33) Is procedure/program documentation relative to the payment process treated as highly sensitive data and safeguarded when superseded?

34) Are backup files current and securely stored off-site?

35) Are re-runs checked for the possibility of fraud, especially duplicate payments?