Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

CMS Security Whitepaper:

Security Configuration Templates

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *SECURITY CONFIGURATION TEMPLATES,* VERSION 2.0

1) Updated the baseline version with the CMS style format.
2) Section 1: Changed controls to security requirements.
3) Section 2: Deleted quotes from this document that is not in the current version of the BPSSM.
4) Section 4: Added the quote from the BPSSM that STIGs are mandatory.
   a) Change the security requirements listed in the BPSSM to the ARS to include the CMSRs.
5) Table 2: Includes applicable FISCAM controls and CMSRs.
6) Table 3: Deleted.

SUMMARY OF CHANGES IN *SECURITY CONFIGURATION TEMPLATES,* VERSION 1.0

1) Baseline Version 1.0.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

(This Page Intentionally Blank)

1 INTRODUCTION

One aspect of effective information technology (IT) security requirements validation is based on a foundation of comprehensive Federal Information Systems Controls Audit Manual (FISCAM) controls in the development and implementation of an entitywide security program.

This whitepaper will:

- provide a high level understanding of the development and implementation of the security configuration templates,
- facilitate the identification of IT controls, in key federal guidelines and standards, which are directly related to the development and implementation of security configuration templates, and
- provide a sample of prior instances of non-compliance with the CMSRs and recommended possible corrective measures.

2 INTRODUCTION TO THE IMPLEMENTATION AND MAINTENANCE OF SECURITY CONFIGURATION TEMPLATES

The General Accounting Office' (GAO) *Federal Information Systems Controls Audit Manual (FISCAM) Exposure Draft* defines configuration management as:

> "The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system."[1]

NIST has produced Special Publication 800-70[2] *Security Configuration Checklists Program for IT Products - Guidance for Checklist Users and Developers* to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products. NIST SP 800-70 states:

> "A security configuration checklist (also called a lockdown, hardening guide, or benchmark) is a series of instructions for configuring a product to a particular operational environment."

It could also include templates or automated scripts and other procedures to apply these settings. Checklists can be created by IT vendors for their own products or created by other organizations such as consortia, academia, open source, and government agencies. The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products.

[1] The General Accounting Office' (GAO) *Federal Information Systems Controls Audit Manual (FISCAM)* Exposure Draft, date July 2008.

[2] Special Publication 800-70 *Security Configuration Checklists Program for IT Products - Guidance for Checklist Users and Developers,* Rev 1 Draft dated September 2008.

3 RISKS OF NON-COMPLIANCE

In discussing security configuration templates and checklists, NIST 800-70 also states that:

> "Vulnerabilities in IT products are discovered daily,1 and many ready-to-use exploitation techniques are widely available on the Internet. Because IT products are often intended for a wide variety of audiences, restrictive security configuration controls are usually not enabled by default, so many out-of-the-box IT products are immediately vulnerable."

Some of the risks inherent in not implementing and maintaining common security templates include:

- the inconsistent application of security configurations across all vulnerable platforms could cause a single system to be compromised and serve as an entry point to the larger network,
- lack of common security configuration standards would increase the time required to research and apply security settings to systems individually.

The potential consequences of inconsistent or lack of use of security configuration templates or checklists are identical to those associated with inadequate access controls, which are indicated in FISCAM.

4 SPECIFIC REQUIREMENTS TO BE IMPLEMENTED

Security configuration templates take one of two forms. Some configuration templates are software-based in the form of a file or files which contain predetermined security settings which can be applied to single or multiple systems in an automated fashion. The NIST Information Security Automation Program (ISAP) (http://nvd.nist.gov/scap.cfm) is a good example of these. The ISAP is a U.S. government multi-agency initiative to enable automation and standardization of technical security operations. The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). NVD is the U.S. government content repository for ISAP and SCAP.

The other type of configuration template is policy-based and in the form of a checklist recommendations guide, or baselines, applied manually to the system during initial build and deployment.

Both NIST and the NSA provide security configuration checklists and security configuration guides for multiple operating systems and applications. Additionally, Security Technical Implementation Guides (STIGs) are published as tools to assist in the improvement of the security of Department of Defense (DOD) information systems. They are created using the principle that the most effective way to improve security in information systems is to include security in the initial design and development. As such, they provide the technical security policies, requirements, and implementation details for applying security concepts to information systems.

CMS highly encourages business partners to utilize these and other guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

The use of STIGs and other configuration standards and templates will:

- Reduce the likelihood of successful intrusions or attacks;
- Facilitate secure configuration of systems prior to network deployment;
- Assist with monitoring systems for on-going conformance with security configurations

Some operating system vendors include robust configuration management capabilities within the software. For example, Microsoft has included multiple methods to natively manage the configuration of Windows systems. The Windows Security Configuration Manager tool set allows administrators to create, apply and edit the security for local computers, organizational units, or domains. Windows also allows the construction and application of software-based security configuration templates. Microsoft states,

> "With the Security Templates snap-in for Microsoft Management Console, administrators can create a security policy for computers or for networks. It is a single point of entry where the full range of system security can be taken into account. The Security Templates snap-in does not introduce new security parameters; it simply organizes all existing security attributes into one place to ease security administration."

Security guidelines and security configuration checklists 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. Checklists are a tool that provide detailed instructions for checking the presence of a vulnerabilities (that result from poorly configured environments) identified in a STIG. Both are developed by NSA, DISA, and NIST to help system operators configure security within their systems to the highest level possible. All STIGs and Checklists are available at no cost from DISA. The link for STIGs is: http://iase.disa.mil/stigs/stig/index.html, and the link for Checklists is: http://iase.disa.mil/stigs/checklist/index.html. CMS highly recommends that business partner SSOs (or their designated representative) subscribe to the DISA STIG-News Mailing List at: http://iase.disa.mil/help/mailing-list.html so they will be notified whenever updated or new STIGs become available.

The use of STIGs is mandatory for all business partner systems/applications that process, store, and/or transmit Medicare claims data. DMEMACs, ABMACs, and EDCs are required to start with the STIG baseline configurations and then document any exceptions based on environment specific implementation. 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 feasible, and to implement all settings that are found to be feasible. All STIG recommended security settings that are determined not to be feasible in a business partner environment shall be documented in the applicable system/application IS RA with appropriate justification.

Security Configuration Templates

To assist business partners in implementing STIG security settings, there are several CMS Security Guides available for the more common systems/applications used in the business partner environment. These guides are available through the CMS IS "Virtual Handbook" Web site at: http://www.cms.hhs.gov/InformationSecurity/.

NSA has also developed and distributed configuration guidance for a wide variety of software from open-source to proprietary. The objective of the NSA configuration guidance program is to provide administrators with the best possible security options in the most widely used products. NSA provides these guidelines at: http://www.nsa.gov/snac/downloads_all.cfm.

The Center for Internet Security (CIS) provides security configuration benchmarks that represent a prudent level of due care, and are working to define consensus best-practice security configurations for computers connected to the Internet. CIS scoring tools analyze and report system compliance with the technical control settings in the benchmarks. The CIS benchmarks and scoring tools are available for download at: http://www.cisecurity.com/benchmarks.html.

The BPSSM states that “Business partners are required to perform an annual risk assessment in accordance with the CMS Information Security RA Methodology.” The relevant FISCAM and CMSRs identified to mitigate the risks discovered in the risk assessment can then be used to develop effective security configuration templates. Additionally, the BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

All requirements documented in the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* (CMSR) are mandatory and must be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as ‘guidance’ and as such some controls may not apply to specific IT environments within CMS. In these cases, business partners must develop clear and concise reasoning. Barring such exceptions, all security requirements are deemed applicable, unless other compensatory security requirements are in place, which satisfy the security requirement objective.

Table 2 lists all the applicable change management and monitoring controls specific to a FISCAM audit and related CMSRs respectively. Refer to chapters three (3) and four (4) of FISCAM for the “Control Techniques” and “Audit Procedures” for each “Control Activity” listed in Table 2. Refer to the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* for a more detailed discussion of each CMSR in Table 2.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific “Control Enhancements”, within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare claims processing systems and Medicare data center systems be categorized as “high impact” security systems.

As mentioned above, Table 2 contains a listing of all FISCAM controls listed in the FISCAM which are applicable to change management.

In order to provide further detailed guidance on specific controls for each FISCAM critical element the reader can then refer to chapters three (3) or four (4) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements*, CMS has outlined the mandatory CMSRs which need to be in place in every information system that processes or stores Medicare-related data. Business partners must establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CMSRs within the body of the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* document. The CMSRs are organized into seventeen families and three (3) classes, as described in the CMSR document.

CMS management is committed to ensuring that each version of the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* and the BPSSM (current and future versions) includes the applicable FISCAM and CMSRs discussed above in order to facilitate full compliance with guidelines related to the implementation and maintenance of security configuration templates.

5 SAMPLE INSTANCES OF NON-COMPLIANCE AND RECOMMENDED RESOLUTION

Table 1 provides a listing of sample instances of non-compliance with the implementation and maintenance of security configuration templates and checklists based on prior controls reviews and audits. Specifically, the table lists the findings and recommended course of action for selected cases of non-compliance. In these cases non-compliance refers not only to controls which were not in place, but also to controls which may have been applied if security configuration templates had been used to configure those systems. The findings in Table 1 are not exhaustive in that they do not list ALL prior instances of non-compliance at all CMS sites. A sample of prior audit findings and issues have been selected instead in order to give the reader a sense of "real world" cases of prior control issues found at various CMS locations while avoiding repetition of similar issues found at different CMS sites. It should also be noted that the recommendation for each issue take into account the business operations and technology environment of a specific CMS site. Consequently, the recommendation listed in the table for a specific issue may not apply to all sites.

Table 1 Sample Findings from Prior CMS Controls Reviews and Audits

Finding	Issue	Suggested Remediation
Default or blank passwords exist for user accounts.	Malicious users could gain the ability to gain access to systems.	Unique passwords should be created for each account.
The rlogin service is enabled.	The r-services, in conjunction with the /etc/hosts.equiv file and individual rhosts files, place a system at risk. They allow users to log in or execute commands from a	The Berkley r-services (e.g., rexec, rlogin, rsh) should be disabled unless there is a strong business need. One

Finding	Issue	Suggested Remediation
	trusted system without re-authenticating.	potential alternative is to use SSH for remote access.
The Simple Mail Transport Protocol (SMTP) service appears to allow relaying.	Mail servers should not allow relaying as this could allow the server to be used to falsify e-mails or send SPAM, potentially opening the organization up to liability.	Disable SMTP if not needed or configure to disallow relaying for any users not coming from organization-owned networks.
There are users whose passwords never expire. In addition, some users cannot change their passwords.	This setting is not recommended unless this is a service account, as it leads to less frequent password changes	Enable the setting to make these users change their passwords on a regular basis. Remove the Password Never Expires option
The minimum password length, maximum password age, password history length, and minimum password age are not set accordance with policy	Insufficient password policies can allow attackers to compromise accounts with weak passwords.	If a password policy does not currently exist, a strong, enterprise wide password policy should be developed. This password policy should be enforced on all servers and applications in the environment.
Multiple default Microsoft Internet Information Services (IIS) files that result in exposing system information are present on the system.	These files may provide sensitive information about medical clients, usernames, and passwords or allow files to be written to the system.	Less secure default settings should be changed for all applicable systems. All unnecessary services and applications should be removed.
Unsecured network services, such as Telnet and FTP are enabled.	Passwords are transmitted across the network in clear text when a user is logging into these services and could be obtained by a malicious user.	Unnecessary services should be removed or disabled when not in use. Encryption of logins and passwords should be enabled wherever possible.
Web pages containing system information do not require authentication.	Browsing of sensitive web pages which do not require authentication may provide sensitive information to compromise the host.	Access to sensitive information should be restricted to authorized users only.
Null sessions were established with numerous Windows systems.	If not appropriately restricted, null sessions may allow an unauthorized user to obtain sensitive information, including user names and system information.	Null sessions should have restrictions placed on their use, including but not limited to restricted access, session timeouts, and access logging.
A default version of Microsoft SQL Server 2000 is installed.	Microsoft SQL Server 2000 is vulnerable to a heap buffer overflow in the SQL Server Resolution Service, which is used to direct client requests to the proper port when multiple instances of the SQL Server are running on the same system. By sending a specially-crafted request to UDP port 1434 consisting of a byte set to 0x08 followed by an overly long string and a colon character (:), a remote attacker could overflow a buffer	All affected servers should be patched for this vulnerability, as listed in Microsoft Security Bulletin MS02-039. Recommend upgrading SQL Server 2000 to the most recent Microsoft SQL Server release.

Finding	Issue	Suggested Remediation
	and cause the SQL Server service to crash or execute arbitrary code on the system with the same privileges as the SQL Server.	

6 PERIODIC REVIEW AND TESTING OF CONTROLS

Computers and the environments in which they operate are dynamic. Business process needs, supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security requirement needs an assurance mechanism to ensure effectiveness. Refer to *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* (CMSR) for guidance on assurance mechanisms for CMS information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls must be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls. Additionally, the BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* must be reviewed and modified on an on-going basis to ensure compliance with updates to Federal standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

FISCAM refers to the maintenance of security configuration templates more specifically when it discusses maintaining System Security Plans. It states,

> “To be effective, the policies and plan should be maintained to reflect current conditions. They should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in agency mission or the types and configuration of computer resources in use. Revisions to the plan should be reviewed, approved, and communicated to all employees. Outdated policies and plans not only reflect a

> lack of top management concern, but also may not address current risks and, therefore, may be ineffective.”

The BPSSM states that “CMS does require that an active configuration management program be established and maintained, including the development/use of configuration standards within the entity.” As requirements change or arise from the configuration management program, these new changes should be reflected by changes in the appropriate template.

7 CONCLUSION

According to NIST, while the use of security configuration checklists and templates can greatly improve overall levels of security in organizations, no checklist can permit a system or a product to become 100 % secure. However, use of checklists and templates that emphasize hardening of systems against flaws or bugs inherent in software will typically result in greater levels of product security and protection from future threats.

The threats facing networks today are dynamic and persistent. New systems not only need to be secure before becoming operational, but the standards used to configure them also need to be continually updated to keep pace with new and changing threats.

The implementation of these controls should be part of an enterprise-wide operational approach rather than a technology-centric approach and should, thus, be incorporated in the highest levels of management planning and enforcement practices within CMS. This, of course, necessitates the direct involvement of management at the highest levels of the organization (not just technology management).

Given the dynamic nature of CMS’ operational needs and the technology supporting these needs, the re-assessment, modification and re-design of CMS’ security management and control practices as well as the testing and monitoring of compliance with these practices must be an on-going process to ensure new operational and technology developments and the resulting security vulnerabilities are effectively addressed.

Table 2 provides applicable FISCAM controls and CMSRs for guidance in the use of security configuration templates.

Table 2 Applicable FISCAM Controls[3]

FISCAM Critical Elements	CMSR Description
AC-3 Implement effective authorization controls	• AC-13 Supervision and Review - Access Control • AC-14 Permitted Actions without Identification or Authentication • AC-2 Account Management • AC-3 Access Enforcement • AC-6 Least Privilege • AU-2 Auditable Events

[3] The General Accounting Office’ (GAO) *Federal Information Systems Controls Audit Manual (FISCAM)* Exposure Draft, date July 2008.

FISCAM Critical Elements	CMSR Description
	• AU-6 Audit Monitoring, Analysis, and Reporting • CM-6 Configuration Settings • CM-7 Least Functionality • IA-4 Identifier Management • SC-14 Public Access Protections • SC-15 Collaborative Computing • SC-6 Resource Priority
AC-4 Adequately protect sensitive system resources	• AC-1 Access Control Policy and Procedures • AC-15 Automated Marking • AC-16 Automated Labeling • AC-17 Remote Access • AC-18 Wireless Access Restrictions • AC-2 Account Management • AC-3 Access Enforcement • AC-6 Least Privilege • AU-2 Auditable Events • AU-6 Audit Monitoring, Analysis, and Reporting • CM-5 Access Restrictions for Change • IA-4 Identifier Management • IA-7 Cryptographic Module Authentication • MA-3 Maintenance Tools • MA-4 Remote Maintenance • MP-2 Media Access • MP-3 Media Labeling • MP-4 Media Storage • MP-5 Media Transport • MP-6 Media Sanitization and Disposal • PE-19 Information Leakage • SC-11 Trusted Path • SC-12 Cryptographic Key Establishment and Management • SC-13 Use of Cryptography • SC-16 Transmission of Security Parameters • SC-18 Mobile Code • SC-2 Application Partitioning • SC-3 Security Function Isolation • SC-4 Information Remnance • SC-8 Transmission Integrity • SC-9 Transmission Confidentiality • SC-CMS-3 • SC-CMS-4 • SI-7 Software and Information Integrity

Security Configuration Templates

FISCAM Critical Elements	CMSR Description
AS-3 Implement effective application configuration management	• AC-3 Access Enforcement • AC-5 Separation of Duties • AC-6 Least Privilege • CA-2 Security Assessments • CM-3 Configuration Change Control • CM-4 Monitoring Configuration Changes • CM-5 Access Restrictions for Change • CM-6 Configuration Settings • SA-10 Developer Configuration Management • SA-11 Developer Security Testing • SA-3 Life Cycle Support • SA-5 Information System Documentation • SI-2 Flaw Remediation • SI-5 Security Alerts and Advisories
CM-1 Develop and document CM policies, plans, and procedures	• CM-1 Configuration Management Policy and Procedures • SA-3 Life Cycle Support
CM-2 Maintain current configuration identification information	• CM-2 Baseline Configuration • CM-6 Configuration Settings • CM-8 Information System Component Inventory • SA-5 Information System Documentation
CM-3 Properly authorize, test, approve, and track all configuration changes	• AC-3 Access Enforcement • CM-2 Baseline Configuration • CM-3 Configuration Change Control • CM-4 Monitoring Configuration Changes • CM-5 Access Restrictions for Change • CM-6 Configuration Settings • CM-7 Least Functionality • SA-10 Developer Configuration Management • SA-11 Developer Security Testing • SA-2 Allocation of Resources • SA-3 Life Cycle Support • SA-4 Acquisitions • SA-5 Information System Documentation • SA-7 User Installed Software • SA-8 Security Engineering Principles
CM-4 Routinely monitor the configuration	• CM-4 Monitoring Configuration Changes • CM-5 Access Restrictions for Change • SA-10 Developer Configuration Management • SI-6 Security Functionality Verification • SI-7 Software and Information Integrity

FISCAM Critical Elements	CMSR Description
CM-5 Update software on a timely basis to protect against known vulnerabilities	• CM-2 Baseline Configuration • CM-3 Configuration Change Control • MA-1 System Maintenance Policy and Procedures • PL-3 System Security Plan Update • RA-4 Risk Assessment Update • RA-5 Vulnerability Scanning • SA-6 Software Usage Restrictions • SA-7 User Installed Software • SC-1 System and Communications Protection Policy and Procedures • SC-19 Voice Over Internet Protocol • SI-2 Flaw Remediation • SI-3 Malicious Code Protection • SI-5 Security Alerts and Advisories • SI-8 Spam Protection
CM-6 Appropriately document and approve emergency changes to the configuration	• CM-3 Configuration Change Control • SA-10 Developer Configuration Management
CP-3 Develop and document a comprehensive contingency plan	• CP-1 Contingency Planning Policy and Procedures • CP-10 Information System Recovery and Reconstitution • CP-2 Contingency Plan • CP-5 Contingency Plan Update • CP-6 Alternate Storage Site • CP-7 Alternate Processing Site • CP-8 Telecommunications Services • SA-3 Life Cycle Support
DA-1 Implement an effective data management system strategy and design	• AC-4 Information Flow Enforcement • AU-2 Auditable Events • AU-3 Content of Audit Records • AU-5 Response to Audit Processing Failures • AU-6 Audit Monitoring, Analysis, and Reporting • SA-10 Developer Configuration Management • SA-3 Life Cycle Support • SA-5 Information System Documentation • SC-2 Application Partitioning • SI-4 Information System Monitoring Tools and Techniques • SI-5 Security Alerts and Advisories
IN-1 Implement an effective interface strategy and design	• SA-3 Life Cycle Support • SA-5 Information System Documentation • SI-10 Information Accuracy, Completeness, Validity, and Authenticity • SI-11 Error Handling

FISCAM Critical Elements	CMSR Description
	• SI-9 Information Input Restrictions
SM-1 Establish a security management program	• AC-1 Access Control Policy and Procedures • AT-1 Security Awareness and Training Policy and Procedures • AU-1 Audit and Accountability Policy and Procedures • CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures • CA-3 Information System Connections • CM-1 Configuration Management Policy and Procedures • CM-8 Information System Component Inventory • CP-1 Contingency Planning Policy and Procedures • IA-1 Identification and Authentication Policy and Procedures • IR-1 Incident Response Policy and Procedures • MA-1 System Maintenance Policy and Procedures • MP-1 Media Protection Policy and Procedures • PE-1 Physical and Environmental Protection Policy and Procedures • PL-1 Security Planning Policy and Procedures • PL-2 System Security Plan • PL-3 System Security Plan Update • PL-6 Security-Related Activity Planning • PS-1 Personnel Security Policy and Procedures • PS-CMS-2 • RA-1 Risk Assessment Policy and Procedures • SA-1 System and Services Acquisition Policy and Procedures • SA-2 Allocation of Resources • SC-1 System and Communications Protection Policy and Procedures • SI-1 System and Information Integrity Policy and Procedures
SM-3 Document security control policies and procedures	• AC-1 Access Control Policy and Procedures • AT-1 Security Awareness and Training Policy and Procedures • AU-1 Audit and Accountability Policy and Procedures • CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures • CM-1 Configuration Management Policy and Procedures • CP-1 Contingency Planning Policy and Procedures • IA-1 Identification and Authentication Policy and Procedures • IR-1 Incident Response Policy and Procedures • MA-1 System Maintenance Policy and Procedures • MP-1 Media Protection Policy and Procedures • PE-1 Physical and Environmental Protection Policy and Procedures • PL-1 Security Planning Policy and Procedures • PS-1 Personnel Security Policy and Procedures • RA-1 Risk Assessment Policy and Procedures

FISCAM Critical Elements	CMSR Description
	• SA-1 System and Services Acquisition Policy and Procedures • SC-1 System and Communications Protection Policy and Procedures • SI-1 System and Information Integrity Policy and Procedures
SM-5 Monitor the effectiveness of the security program	• AU-6 Audit Monitoring, Analysis, and Reporting • CA-2 Security Assessments • CA-4 Security Certification • CA-5 Plan of Action and Milestones • CA-6 Security Accreditation • CA-7 Continuous Monitoring • CM-4 Monitoring Configuration Changes • IR-5 Incident Monitoring • PE-6 Monitoring Physical Access • PL-5 Privacy Impact Assessment • RA-5 Vulnerability Scanning • SA-11 Developer Security Testing • SI-4 Information System Monitoring Tools and Techniques • SI-5 Security Alerts and Advisories

(This Page Intentionally Blank)