CMS Manual System	**Department of Health & Human Services (DHHS)**
Pub 100-17 Medicare Business Partners Systems Security	**Centers for Medicare & Medicaid Services (CMS)**
Transmittal 11	**Date: September 30, 2011**
	Change Request 7328

SUBJECT: CMS Business Partners Systems Security Manual

I. SUMMARY OF CHANGES: The purpose of this update is to communicate to Medicare Contractors changes to CMS and NIST requirements and procedures.

EFFECTIVE DATE: October 31, 2011
IMPLEMENTATION DATE: October 31, 2011

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
R	1/Introduction
R	1/1/Additional Requirements for MACs
R	2/1/CMS Contract Officer Technical Representative (COTR)
R	3/IT Systems Security Program Management
R	3/1/System Security Plan (SSP)
R	3/2/Risk Assessment
R	3/3/Certification
R	3/4/Information Technology (IT) Systems Contingency Plan
R	3/5.1/Annual FISMA Assessment (FA)
R	3/5.2/Plan of Action and Milestones (POAandM)
R	3/5.2.1/Background
R	3/5.2.2/POAandM Package Components/Submission Format
R	3/5.3/Annual/Yearly Compliance Condition
R	3/6.1/Computer Security Incident Response
N	3/8/Authorization To Operate
R	3/9/Fraud Control
R	3/10/Patch Management
R	3/11/Security Management Resources
R	3/11.1/Security Configuration Management
R	3/11.2/Security Technical Implementation Guides (STIG)
R	3/11.3/DHHS Federal Desktop Core Configuration (FDCC) Standard
R	3/11.4/National Institute of Standards and Technology (NIST)
R	4/1.1/Potential Security Impact Level
R	4/1.2/Security Level by Information Type
R	4/1.3/CMS Security Level Designation-HIGH
R	4/1.4/Minimum System Security Requirements-HIGH
R	4/2.7/Minimum Protection Alternatives
R	4/3/Encryption Requirements for Data Leaving Data Centers
R	5/Internet Security
R	Appendix A/12/References
D	Appendix C

III. FUNDING:

For Fiscal Intermediaries (FIs), Regional Home Health Intermediaries (RHHIs) and/or Carriers:
No additional funding will be provided by CMS; Contractor activities are to be carried out within their operating budgets.

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

**Unless otherwise specified, the effective date is the date of service.*

Attachment - Business Requirements

Pub. 100-17	Transmittal: 11	Date: September 30, 2011	Change Request: 7328

SUBJECT: CMS Business Partners Systems Security Manual

Effective Date: **October 31, 2011**

Implementation Date: October 31, 2011

I. GENERAL INFORMATION

A. Background: The purpose of this update is to communicate to Medicare Contractors changes to CMS and NIST requirements and procedures.

B. Policy: The policies mandating this change are the Federal information Security Management Act of 2002, National Institute of Standards and Technology guidance and CMS policies, standards, guidelines and procedures.

II. BUSINESS REQUIREMENTS TABLE

Number	Requirement	Responsibility									
		A/B MAC	DME MAC	FI	CARRIER	RHHI	Shared-System Maintainers				Other
							FISS	MCS	VMS	CWF	
7328.1	Medicare Contractors and Shared System Maintainers shall follow the processes outlined in the Medicare Business Partners Systems Security Manual.	x	x	x	x	x	x	x	x	x	HIGLAS, EDCs, ZPICs
7328.2	Medicare Contractors and Shared System Maintainers shall follow the instructions and guidance when evaluating all CMSRs and preparing CMSR responses.	x	x	x	x	x	x	x	x	x	HIGLAS, EDCs, ZPICs

III. PROVIDER EDUCATION TABLE

Number	Requirement	Responsibility									
		A/B MAC	DME MAC	FI	CARRIER	RHHI	Shared-System Maintainers				Other
							FISS	MCS	VMS	CWF	
	None.										

IV. SUPPORTING INFORMATION

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

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): Jason King 410-786-7578 or Kevin Potter 410-786-5686

Post-Implementation Contact(s): Contact your Contracting Officer's Technical Representative (COTR) or Contractor Manager, as applicable.

VI. FUNDING

Section A: For *Fiscal Intermediaries (FIs), Regional Home Health Intermediaries (RHHIs),* and/or *Carriers*:

No additional funding will be provided by CMS; contractor activities are to be carried out within their operating budgets.

Section B: *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.

Centers for Medicare & Medicaid Services (CMS)

Business Partners

Systems Security Manual

CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

(Rev. 11)

CMS/ Business Partners
Systems Security Manual

Record of Changes

(Rev. 11)

Revision	Major Changes	Date
11	*Main Document and all Appendices:* *(1) CISS references removed throughout document and replaced with CFACTS.* *(2) Changed email to e-mail throughout document.* *(3) Changed CMS POA&M and Annual FISMA Assessment using CISS Guideline to CFACTS Guideline.* *(4) Project Officer (PO) changed to Contract Officer Technical Representative (COTR) throughout document.* *1: Updated grammar and hyperlink to legislative resources document.* *1.1: Evaluation and test changed to security control assessment. Accreditation changed to authorization.* *2.1: Second bullet deleted.* *3: FISMA U.S. Code reference added. Contact addresses updated.* *Table 3.1: CPIC and CFACTS text added. Additional bullets added to 3.6 and 3.8 Authorization to Operate row added.* *3 Legend: CISS line item deleted. CFACTS and COTR added.* *Footnote 5: NIST reference updated.* *3.1: FISMA and Privacy Act reference added. CFACTS text added. SSP hyperlink updated. CyberTyger deleted and e-mail address changed.* *3.2: RA hyperlink updated. Grammar update. CFACTS text added. CyberTyger deleted and e-mail address changed.* *3.3: Bullet text deleted and POA&M reference updated.* *3.4: CFACTS text added.*	*09-30-11*

Revision	Major Changes	Date
	3.5: Grammar update.	
	3.5.1: Updated wording for clarity.	
	3.5.2: CFACTS text added. File changed to report.	
	3.5.2.1: Updated wording for clarity.	
	3.5.2.2: Updated wording for clarity.	
	3.5.3: Updated wording for clarity.	
	3.6.1: CMS hyperlink updated.	
	Table 3.2: CAT 5 name updated to reflect NIST wording. NIST reference updated.	
	3.8: ATO section added. Subsequent sections renumbered accordingly.	
	3.10: CERT hyperlink added. NIST reference updated.	
	3.11.1: added quarterly Baseline Configuration submission info.	
	3.11.2: Hyperlinks updated.	
	3.11.3: Dates deleted. Help desk e-mail address changed.	
	3.11.4: Table 3.4 wording deleted. NIST hyperlink added.	
	Table 3.4: Deleted	
	4.1.1: Table 4.1 wording deleted.	
	Table 4.1: Deleted	
	4.1.2: Updated wording for clarity.	
	Table 4.2: Deleted	
	4.1.3: Table 4.2 reference deleted. CMS System Security and e-Authentication Assurance Levels by Information Type document referenced.	

Revision	Major Changes	Date
	4.1.4: NIST references updated. *Table 4.3: Renamed to Table 4.1.* *4.3: Changed CMS Policy for the Information Security Program (PISP) reference and wording to reflect the most recent version. MP-5(1) control enhancement reference deleted per being moved to MP-5 in NIST 800-53 Rev. 1.* *5: Changed ST&E to Security Control Assessment. Changed C&A to Security Authorization. NIST references updated. Numbering style and format update. Second bullet with hyperlink not working deleted. Internet capitalized.* *Appendix A: References and links updated to reflect most current document available.* *Appendix C: Deleted. References removed throughout document.*	

CMS/Business Partners
Systems Security Manual

Table of Contents

(Rev. 11)

Appendices

(Rev. 11)

1 Introduction

(Rev. 11)

The Centers for Medicare & Medicaid Services (CMS) requires that its business partners implement information security (IS) controls on their information technology (IT) systems to maintain the confidentiality, integrity, and availability (CIA) of Medicare systems' operations in the event of computer incidents or physical disasters.

A CMS business partner (contractor) is a corporation or organization that contracts with CMS to process or support the processing of Medicare fee-for-service claims. These business partners include Medicare carriers, Fiscal Intermediaries (FIs), Common Working File (CWF) host sites, standard system maintainers, regional laboratory carriers, claims processing data centers, Data Centers, Enterprise Data Centers (EDCs), and Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors [DMEMAC] and Part A/Part B Medicare Administrative Contractors [ABMAC]).

The "Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA)- SEC. 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," 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.

This manual addresses the following key business partner security elements:

- 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 found on the CMS IS "Virtual Handbook" Web site at: http://www.cms.hhs.gov/InformationSecurity/

Refer to the following CMS IS "Virtual Handbook" Web page for the key public laws and federal regulations regarding, or that impact, the implementation of federal agency IS programs: *https://www.cms.gov/informationsecurity/downloads/legislative_resource.pdf.*

1.1 Additional Requirements for MACs

(Rev. 11)

MACs are responsible for fulfilling all existing business partner requirements. Additional requirements are specified in Section 912 of the MMA. These additional requirements include the following:

- The contractor shall correct weaknesses, findings, gaps, or other deficiencies within 90 days of receipt of the final audit or evaluation report, unless otherwise authorized by CMS.

  The contractor shall comply with the CMS Information Security (IS) Certification & Accreditation (C&A) Program Procedures, policies, standards, and guidelines for contractor facilities and systems. The CMS IS C&A Program Procedures can be found on the CMS Web site at: http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#

- 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 support CMS validation and *authorization* of contractor systems and facilities in accordance with the CMS IS C&A Program Procedures.

- The contractor shall provide annual certification, in accordance with the CMS IS C&A Program Procedures, that they have examined the management, operational, and technical controls for its systems supporting the MAC function, and consider these controls adequate to meet CMS security standards and requirements.

- The contractor shall appoint a Chief Information Officer (CIO) to oversee its compliance with the CMS IS requirements. The contractor's principal Systems Security Officer (SSO) shall be a full-time position dedicated to assisting the CIO in fulfilling these requirements.

2 IT Systems Security Roles and Responsibilities

2.1 CMS *Contract* Officer *Technical Representative* (*C*O*TR*)

(Rev. 11)

CMS *COTR*s (generally located in CMS Central Office [CO] business components) oversee the other business partners and also have Federal Acquisition Regulation (FAR) responsibilities at data centers. The *COTR* has the following responsibilities:

- CMS point of contact for business partner IS problems
- Provider of technical assistance necessary to respond to CMS IS policies and procedures

3 IT Systems Security Program Management

(Rev. 11)

Business partners shall have policies and procedures, and implement controls or plans that fulfill the CMSRs (see CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#). The business partner Medicare claims related security program shall be based on the collection of CMS policies, procedures, standards and guidelines found on the CMS IS "Virtual Handbook" Web site at: http://www.cms.hhs.gov/InformationSecurity.

Policies are formal, up-to-date, documented rules stated as "shall" or "will" statements that exist and are readily available to employees. They establish a continuing cycle of assessing risk and implementation and use 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.

Controls are measures implemented to protect the CIA of sensitive information. IS procedures and controls shall be implemented in a consistent manner everywhere that the procedure applies. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. In addition, initial testing shall be performed to ensure that IS controls are operating as intended.

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. Business partners shall perform a *Federal Information Security Management Act of 2002, 44 U.S.C. §3541 (*FISMA*)* Assessment[1] (FA) using the *CMS FISMA Controls Tracking System (CFACTS)*. The weaknesses, action plans, and POA&Ms shall be recorded in the *CFACTS* (See *CFACTS Guideline*). To perform the FA, business partners shall conduct a systematic review of the CMSRs using the *CFACTS*. *CFACTS* provides a "Control Response" form that includes guidance and assessment procedures to assist in the review of the CMSRs.

The CMSRs include key security-related tasks. Table 3.1 indicates how often these tasks 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)
CMS POA&M & Annual FISMA Assessment	One third of the controls shall be tested each federal FY so all controls are tested during a 3-year period.	• *COTR* with a copy to CMS CO *via CFACTS* • System Security Profile	See *CFACTS Guideline* for an overview of the FA. FA results recorded *in* the *CFACTS* are to be discussed in the *CPIC* Certification Package.	
3.1 Information Security (IS) System Security Plans (SSP)	The IS SSP for each GSS and MA shall be reviewed, updated, and certified by management each federal FY (minimally), or upon significant change[2].	• SSO • CMS CO *via CFACTS* • System Security Profile	IS SSPs are to be reviewed, updated, and certified by management and indicated as such in both *the CFACTS,* the *CPIC* Certification Package/Statement of Certification, and the System Security Profile[3].	

[1] The former CISS FISMA Evaluation (FE) and Self-Assessment (CAST) have been replaced with the OMB mandated annual FISMA security control assessment (FISMA Assessment [FA]).
[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

Requirement	Frequency	Send To	Comments	Complete (check when complete)
3.2 Information Security Risk Assessment (IS RA)	The IS RA for each GSS and MA shall be reviewed, updated, and certified by management each federal FY (minimally), or upon significant change.[1]	• CMS CO *via CFACTS* • System Security Profile	IS RAs are to be reviewed, updated, and certified by management and indicated as such in *the CFACTS,* the *CPIC* Certification Package/Statement of Certification, and the System Security Profile. The IS RA is submitted with the IS SSP[4].	
3.3 Certification	Each federal FY	• *COTR* with a copy to CMS CO *via CFACTS* • System Security Profile	FIs and carriers should include a statement of certification as part of their CPIC package. Each year CMS will publish in Chapter 7 (Internal Controls) of its Financial Management Manual (Pub 100-6) 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 *COTR*s.	
3.4 IT Systems Contingency Plan (CP)	CPs shall be reviewed, updated, and certified by management each federal FY (minimally), or upon significant change.[1] CPs shall be tested annually.	• SSO • CMS CO *via CFACTS* • System Security Profile	Management and the SSO shall approve the CP. The IT Systems CP is to be developed (in accordance with Appendix A *and CMS CP procedures*), reviewed, updated, and certified by management—and indicated as such in *the CFACTS, the* Certification Package/Statement of Certification, and the System Security Profile[5].	
3.5 Compliance	Each federal FY	• SSO • *COTR* • CMS CO *via CFACTS* • System Security Profile	POA&M: POA&Ms address findings of internal/external audits/reviews including *annual security assessments*, and, as applicable: SAS 70 audits, CFO controls audits, the Section 912 evaluation, and data center tests and reviews.	
3.6 Incident Reporting and Response	As necessary	• *COTR* • *CMS IT Service desk* • *MCMG Security Mailbox (See JSM/TDL 09323* • System Security Profile	HIPAA also addresses Incident Reporting information.	
3.7 System Security Profile	As necessary	On file with the Principal SSO		

operations (including mission, functions, image or reputation) or agency assets."

[3] More information about system security planning can be found in the CMS Information Security (IS) System Security Plan (SSP) Procedures.

[4] More information about Risk Assessment Reports can be found in the CMS Information Security Risk Assessment (IS RA) Procedures.

[5] 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)
3.8 Authorization To Operate	*As necessary to acquire and maintain a CMS CIO-granted Authorization to Operate.*	*On file with CMS Office of the Chief Information Security Officer, with a copy maintained in the CFACTS.*		

LEGEND:

CFACTS	*CMS FISMA Controls Tracking System*
CFO	Chief Financial Officer
CO	Central Office (CMS)
COTR	*Contract Officer Technical Representative (COTR)*
CP	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
IS	Information Security
IT	Information Technology
MA	Major Application
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SAS	Statement on Auditing Standard
SP	Special Publication (NIST)
SSO	Business Partner Systems Security Officer
SSP	System Security Plan

Note: The documents listed in *T*able 3.1 may be stored as paper documents, electronic documents, or any combination thereof.

When submitting documentation to the CMS CO, Registered Mail™ or its equivalent (signed receipt required) shall be used. For supporting documentation (such as RAs, CPs, SSPs, etc.), only electronic copies in the approved CMS format are required. Paper copies are only required for certification signature pages, certifying the completion of required periodic document development, review, updates, and certification. Contact addresses are as follows:

Program Safeguard Contractors (PSC) *and Zone Program Integrity Contractors (ZPIC)*

- CMS Central Office
  Center for Program Integrity
  Division of Benefit Integrity Management Operations
  Mail Stop C3-02-16
  7500 Security Blvd.
  Baltimore, MD 21244-1850

Common Working File (CWF) and Shared System Maintainers

- CMS Central Office
  Office of Information Services
  Business Application and Management Group

Mail Stop N3-13-27
7500 Security Blvd.
Baltimore, MD 21244-1850

Fiscal Intermediaries /Carriers/ Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors [DMEMAC] and A/B Medicare Administrative Contractors [ABMAC])

- CMS Central Office
  Center for Medicare
  Medicare Contractor Management Group
  Mail Stop S1-14-17
  7500 Security Blvd.
  Baltimore, MD 21244-1850

Data Centers and Enterprise Data Centers (EDC)

- CMS Central Office
  Office of Information Services
  Enterprise Data Center Group
  Mail Stop N1-19-18
  7500 Security Blvd.
  Baltimore, MD 21244-1850

3.1 System Security Plan (SSP)

(Rev. 11)

The objective of an IS 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 an IS SSP. The completion of an SSP is a requirement of *the Federal Information Security Management Act of 2002 (FISMA), Privacy Act of 1974, As Amended,* 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 an 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 SSPs 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, SSPs should be distributed only on a need-to-know basis.

The SSPs shall be available to the SSO and business partner certifying official (normally the Vice President [VP] for Medicare Operations), and authorized external auditors as required. The SSO and Business Owner 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 in accordance with the most current version of the CMS System Security Plan (SSP) procedures available on the CMS Web site at: http://www.cms.hhs.gov/InformationSecurity.

SSPs shall be re-certified within 365 days from the previous certification date. The SSP shall also be reviewed prior to re-certification (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 *recorded in the CFACTS,* placed in the System Security Profile, and a copy shall be submitted to the CMS CO.

Contractors updating their current SSP(s) or developing new SSP(s) shall include Medicare claims processing front-end, back-end, and/or other claims processing related systems using the most current version of the CMS SSP procedures.

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.

A newly developed or updated SSP shall be *maintained in the CFACTS and* sent in electronic form to the CMS CO on CD-ROM. This CD-ROM must be received by CMS 10 working days after the SSP(s) has been developed, updated, or re-certified. The original signed, dated CMS SSP certification form shall be submitted in paper copy form along with the CD-ROM electronic copy. This information shall not be submitted to the CMS CO via *e-mail*—Registered Mail™ or its equivalent (signed receipt required) shall be used.

In summary, the SSP shall be updated and re-certified annually unless there are changes (as discussed above) that would necessitate a more frequent update. Should SSP technical assistance be required, direct all questions to *the CMS Office of the Chief Information Security Officer* at *CISO*@cms.hhs.gov.

3.2 Risk Assessment

(Rev. 11)

Business partners are required to perform an annual risk assessment in accordance with the most current versions of the CMS Information Security Risk Assessment procedures available on the CMS Web site at: http://www.cms.hhs.gov/InformationSecurity.

The CMS IS RA procedures present a systematic approach for the RA process of Medicare information computer systems within the CMS and business partner environments. The procedure describe*s* the steps required to produce an IS RA 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 IS RA procedures shall be used to prepare an annual IS RA.

IS RAs shall be re-certified within 365 days from the previous certification date. The RA shall also be reviewed prior to re-certification (within the original certification timeframe) to determine whether an update is required. The RA 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 RA, if applicable,

shall be placed in the System Security Profile, and a copy shall be submitted to the CMS CO. Note that the RA used to support a SSP cannot be dated more than 12 months earlier than the SSP certification date.

Contractors that must update their current RA(s) shall use the most current versions of the CMS IS RA procedures.

A newly developed or updated RA that is submitted with the SSP shall be *maintained in the CFACTS and* sent to the CMS CO on CD-ROM. The CD-ROM must be received by CMS 10 working days after they have been developed and/or updated. This information shall not be submitted to the CMS CO via *e-mail*—Registered Mail™ or its equivalent (signed receipt required) shall be used.

In summary, the RA shall be updated annually unless there are changes (as discussed above) that would necessitate a more frequent update. Should RA technical assistance be required, direct all questions to *the CMS Office of the Chief Information Security Officer at CISO@cms.hhs.gov*.

3.3 Certification

(Rev. 11)

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 CMSRs. 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 IS compliance within each federal FY. This security certification shall be included in the Certification Package for Internal Controls (CPIC) or, for contracts not required to submit CPICs, send the security certification to their appropriate CMS *COTR*s. 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.

Systems 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)
- Risk Assessment (see section 3.2)
- IT Systems Contingency Plan (see section 3.4 and Appendix A)
- Plan of Action and Milestones (see section 3.5.*2*)

3.4 Information Technology (IT) Systems Contingency Plan

(Rev. 11)

All business partners are required to develop and document an IT Systems Contingency Plan (CP) 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. IT Systems CPs shall be included in management planning and shall be:

- Reviewed whenever new systems are planned or new safeguards contemplated
- Reviewed annually to ensure that they remain feasible
- Tested annually. 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, DMERC]), each individual Medicare contract type shall be tested every year.

Appendix A to this manual provides information on Medicare IT systems contingency planning and testing methods. See *item* 3.4 in Table 3.1, section 3.0, for other references.

Each contractor shall review its IT Systems CP 365 days from the date it was last reviewed and/or updated to determine if changes to the CP are needed. A CP shall be updated if a significant change has occurred. The CP shall also be tested 365 days from the last test performed. 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 IT Systems CP. Information on Medicare IT systems contingency planning can be found in Appendix A.

A newly developed and/or updated IT Systems CP shall be *updated in CFACTS and* submitted to CMS within 10 working days after the business partner's management and SSO have approved it. A copy of the IT Systems CP shall be submitted via CD-ROM to the CMS CO along with a paper copy of the statement of certification. This information shall not be submitted via *e-mail*—Registered Mail™ or its equivalent (signed receipt required) shall be used.

3.5.1 Annual FISMA Assessment (FA)

(Rev. 11)

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 CMSRs 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 CMSRs applicable to a system or application shall be tested. This means a subset (no less than one-third [$^1/_3$]) of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period.

CMS CO reserves the right to mandate which subset of CMSRs must be tested during any given year. CMS *also* require*s* that all CMSRs be tested within a 3-year period. Business Owners, in coordination with the developers/maintainers of CMS applications and systems, are responsible for meeting this requirement.

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 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 CMSR effectiveness. All management-directed and independent testing conducted with 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. 11)

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&M items in the *CFACTS* and, if required by CMS, uploading any additional supporting documentation.

3.5.2.1 Background

(Rev. 11)

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 shall also be 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 reported and included in a periodic POA&M report.

Section 912 of the MMA implemented requirements for annual evaluation, testing, and reporting on security programs for both MACs and existing carrier and FI 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. 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 EDP security-related findings. Security-related finding*s* and approved action plan data is *promptly* entered into the *CFACTS* following all audits/reviews, from which the *CFACTS provides* a single monthly submission *report* that summarizes the current state of security for the business partner.

3.5.2.2 POA&M Package Components/Submission Format

(Rev. 11)

In addition to the initial POA&M reporting that follows each audit/review, summary POA&Ms *will* be *generated* on the 1st of each month*, based on the data maintained in the CFACTS*. The *CFACTS* shall be populated *and maintained* with security-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 the monthly reporting requirements*.

Initial Report. Within 30 days (or as otherwise directed by CMS) of the final results for every internal/external audit/review, an initial CMS POA&M is due to CMS that describes the findings of the audit/review and initial corrective actions planned for implementation.
Monthly POA&M Package. 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 Annual/Yearly Compliance Condition

(Rev. 11)

Many security documents, such as IS RAs, SSPs, Contingency Plans, as well as many CMSR control *requirement*s (see CMS Information Security Acceptable Risk Safeguards *[*ARS*],* CMS Minimum Security Requirements Appendices A, B, and C) require annual or yearly performance (e.g., test, submission, recertification, review, update). When such a requirement is to be performed annually or yearly, it is to be performed no later than the one year anniversary date of its previous performance (i.e., within 365 days [366 days in leap years]). 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.

If the business partner wishes to change the timing cycle of an annual or yearly requirement compliance date, the business partner *is required to* shorten the timing cycle and not lengthen the annual/yearly timing cycle to attain the new performance date. For example, if the annual/yearly performance date for reviewing the SSP is 7/31/06 and the business partner desired to change the review date to 5/31/07, they would be required to review the SSP no later than 7/31/06 and again no later than 5/31/07, and no later than 5/31/yy thereafter.

3.6.1 Computer Security Incident Response

(Rev. 11)

All suspected information security incidents or events shall be reported to the business partner IT service desk (or equivalent business partner function) as soon as an incident comes to the attention of an information system user. All confirmed security incidents and events shall be reported to the CMS IT Service Desk in accordance with the procedures set forth in the CMS Information Security Incident Handling and Breach Analysis/Notification Procedure. This document is available on the CMS Web site at

http://www.cms.hhs.gov/InformationSecurity. The CMS IT Service Desk can be contacted by telephone at 410-786-2580 or by e-mail at: CMS_IT_Service_Desk@cms.hhs.gov.

All CMS contractors and business partners shall utilize the following incident categories, Table 3.2, and reporting time criteria, Table 3.3, when reporting incidents to CMS.

Table 3.2. Incident Categories

Category	Name	Description
CAT 0	Exercise /Network Defense Testing	Used during state, federal, national, international exercises, and approved activity testing of internal/external network defenses or responses.
CAT 1	Unauthorized Access*	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
CAT 2	Denial of Service*	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
CAT 3	Malicious Code*	A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.
CAT 4	Inappropriate Usage*	A person violates acceptable computing use policies.
CAT 5	*Scans/Probes/ Attempted Access*	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.
PII	Personally Identifiable Information (PII) Exposure	Any information about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual. Any incident that involves compromised PII must be reported within 1 hour of detection regardless of the incident category reporting timeframe.

*Source: NIST SP 800-61 *Rev. 1*

Table 3.3. Incident Reporting Timeframe Criteria

Category	Reporting Timeframe
CAT 0	Not applicable; this category is for CMS' internal use during exercises.
CAT 1	Within one hour of discovery/detection.
CAT 2	Within two hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Daily; within one hour of discovery/detection if widespread across agency.
CAT 4	Weekly.
CAT 5	Not applicable; this category is for classified systems.
CAT 6	Not applicable; this category is for CMS' use to categorize a potential incident that is currently being investigated.
PII	Within one hour of discovery/detection.

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 effected 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 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 Senior Information Systems Security Office.

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 risk assessment. Business partners shall refer to The CMS Information Security Incident Handling and Breach Analysis/Notification Procedure for further guidance.

3.7 System Security Profile

Consolidate security documentation (paper documents, electronic documents, or a combination) into a System Security Profile that includes the following items:

- Completed FAs
- IS System Security Plans (for each GSS and MA)
- IS Risk Assessments
- Certifications
- IT Systems Contingency Plans

- POA&Ms for each compliance security review
- POA&Ms for other security review undertaken by DHHS OIG, CMS, Internal Revenue Service (IRS), GAO, consultants, subcontractors, and business partner security staff
- Incident reporting and responses
- Systems IS 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. 11

Business partners are required to acquire and maintain a CMS CIO-issued Authorization to Operate (ATO) for each GSS and MA. The guide for Authorization To Operate is defined in the CMS IS Authorization To Operate Package Guide document, located at: https://www.cms.gov/informationsecurity/downloads/ATO_Package_Guide.PDF.

3.*9* Fraud Control

(Rev. 11)

Business partners are required to safeguard systems against fraud. The CMSRs address fraud control issues such as personnel screening, separation of duties, rotation of duties, and training. Business partners should practice fraud control in accordance with the CMSRs and Appendix B, An Approach to Fraud Control.

3.*10* Patch Management

(Rev. 11)

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. The Computer Emergency Response Team (CERT)/Coordination Center (CC)

(http://www.cert.org) estimates that 95 percent of all network intrusions could be avoided by keeping systems up-to-date with appropriate 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 CMSRs provide specific guidance on time frames for implementing patches.

NIST SP 800-40 *Version 2.0*, 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.

3.1*1* Security Management Resources

3.1*1*.1 Security Configuration Management

(Rev. 11)

FISMA requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them. CMS highly encourages 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.

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 all security configuration guidelines is as follows:

1. CMS
2. DHHS
3. OMB
4. NIST
5. DISA

(Note: DMEMACs, ABMACs, and EDCs are responsible for starting their security configurations with the DISA STIG Checklists)

If there are any questions or concerns about resolving conflicts among security configuration guidelines, business partner SSOs shall contact their CMS Business Owner.

3.*11*.2 Security Technical Implementation Guides (STIG)

(Rev. 11)

Security guidelines, called STIGs, and security configuration checklists, called 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 vulnerability identified in a STIG and configuring detailed system/application configuration settings. Both are developed by DISA to help system operators configure security within their systems to the highest level possible. All STIGs and Checklists are available from DISA. The link for STIGs and checklists is http://iase.disa.mil/stigs/checklist/index.html. CMS 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 STIG Checklists become available.

The use of latest publically available DISA STIG Checklists 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 and/or deviations 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. Settings that cannot be implemented on specific systems shall be documented as “system exceptions,” and settings that cannot be implemented across an entire platform (e.g. Windows 2003, AIX) shall be documented as “system deviations.” 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 Security Configuration Checklist (SCC) with appropriate business justification (security impact, operational impact, business impact), mitigating or compensating controls, and residual risk.

Additional information is available through the CMS IS "Virtual Handbook" Web site at: http://www.cms.hhs.gov/InformationSecurity/.

3.*11*.3 DHHS Federal Desktop Core Configuration (FDCC) Standard

(Rev. 11)

The DHHS is responsible for implementing and administering an information security and privacy program to protect its information resources. The DHHS must be compliant with applicable public laws, Federal regulations, and Executive Orders, including FISMA; OMB Circular A-130, Management of Federal Information Resources, and HIPAA. To meet these requirements, DHHS instituted the DHHS Information Security Program Policy and the DHHS Information Security Program Handbook documents.

The DHHS developed applicable DHHS FDCC Standards for Windows in response to OMB Memorandum (M)-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems. In collaboration with its Operating Divisions (OPDIVs), DHHS developed the standard by testing the original FDCC standard provided by NIST, and making appropriate adjustments to best suit the DHHS and its OPDIV's environment. The resulting DHHS FDCC Standards must be implemented at each OPDIV (i.e., CMS) and its contractor computers that are owned or operated by a contractor on behalf of, or for, the OPDIV, or are integrated into a Federal system subject to FDCC.

The DHHS considers the DHHS FDCC Standards for Windows documents "sensitive" so that they are not publicly available. To obtain a copy of the DHHS FDCC Standards, the designated Systems Security Officer (SSO) from each business partner must request a copy via the *CISO* Help Desk *(CISO@cms.hhs.gov)*. CMS expects business partners to request copies and comply with the DHHS FDCC Standards for Windows.

3.*11*.4 National Institute of Standards and Technology (NIST)

(Rev. 11)

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, as a government agency, 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.

Special 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 for 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 BPSSM and the CMSRs. 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.

CMS continues to work closely with NIST in the development of new standards, FIPS, and security documentation to ensure the highest and most reasonable level of security of Medicare data.

4.1.2 Security Level by Information Type

(Rev. 11)

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.

CMS has defined *many* information types processed on and/or by CMS information systems. *These information types are defined in the CMS System Security and e-Authentication Assurance Levels by Information Type document, located at: http://www.cms.gov/informationsecurity/downloads/ssl.pdf*. 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., CMSRs).

4.1.3 CMS Security Level Designation—HIGH

(Rev. 11)

Although the confidentiality and integrity of some information types (i.e., security categorization [SC]) processed, stored, and/or transmitted on CMS business partner and data center systems could be considered to be at a "Moderate" security level based on the explanations and examples *in the CMS System Security and e-Authentication Assurance Levels by Information Type document*, CMS has designated all Medicare claims-related information to be "Mission-critical information." Consequently, all CMS business partner and data center information systems shall be designated at a "HIGH" system security level.

Business partner system managers and system maintainers/developers shall ensure that their Medicare claims-related information and information systems are accessed only by authorized users. The business partner managers of compartmentalized systems shall take special care to specify the appropriate level of security required when negotiating with GSSs and MAs for services. The "HIGH" security level designation determines the minimum security safeguards (i.e., CMSRs) required to protect sensitive data and to ensure the operational continuity of mission-critical data processing capabilities.

The "HIGH" security level designation applies to both user information and system information, and it is applicable to information in both digital and non-digital form. System information (e.g., network routing tables, password files, and cryptographic key management information) shall be protected at the same level to ensure information and information system CIA.

4.1.4 Minimum System Security Requirements—HIGH

(Rev. 11)

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 NIST SP 800-53 *Rev. 3* (as amended), 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 *Rev. 3*.

This allows agencies, such as CMS, to adjust the security controls to more closely fit its mission requirements and operational environments.

The CMS Policy for the Information Security Program (PISP) individual policy statements, along with the CMS Minimum Security Requirements Procedure security standards 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, form the basis for the CMSRs.

4.2.7 Minimum Protection Alternatives

(Rev. 11)

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

4.3 Encryption Requirements for Data Leaving Data Centers

(Rev. 11)

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.

Effective immediately, and until further notice, 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. The encryption requirement may only be waived through written concurrence from the Business Owner of the data followed by a "wet" signature from the CMS CIO, Deputy CIO, or the Chief Technology Officer (CTO).

The **only** exception to this requirement is for tapes destined for off-site storage or for the purpose of data center transitions, and that data must be shipped using proper precautions (i.e., locked in sturdy containers).
This protected health information (PHI) data protection requirement, published in CIO Directive 07-01 dated June 12, 2007, is in accordance with:

- CMS Policy for the Information Security Program (PISP) section *4.1.10*, Media *Protection*: *Information system media, both digital and non-digital must be protected by: (i) limiting access to information on information system media to authorized users; and (ii) sanitizing or destroying information system media before disposal or release for reuse.*

- CMS Minimum Security Requirements (CMSRs):

    - MP-5: All sensitive information stored on digital media are protected during transport outside of controlled areas by using cryptography and tamper proof packaging and (a) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (b) if shipped, trackable with receipt by commercial carrier. If the use of cryptography is not technically feasible or the sensitive information is stored on non-digital media, written management approval (one level below the CIO) must be obtained prior to transport and the information must be (a) hand carried using securable container via authorized personnel, or (b) if shipped, by United States Postal Service (USPS) Certified Mail with return receipt in tamper-proof packaging. Correspondence pertaining to a single individual may be mailed through regular USPS mail, but should contain the minimal amount of sensitive information in order to reduce the risk of unauthorized disclosure.

    - MP-5(2): Activities associated with the transport of sensitive information system media are documented.

    - MP-5(3): For systems designated at a "HIGH" sensitivity level, employ an identified custodian at all times to transport information system media.

5 Internet Security

(Rev. 11)

With prior written approval of their sponsoring CMS Business Owner, business partners may now use Internet technology for transmission of and/or receipt of health care transactions. Each request for using Internet technology 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) *Security Control Assessment* of the new functionality prior to its release into production is required and the *Security Control Assessment* must include penetration testing. The *Security Control Assessment* is conducted to validate compliance with the following specific architectural, security, data interchange, and privacy requirements, as well as the CMSRs. The *Security Control Assessment* must be conducted by a CMS-contracted third party. The existing requirement for an annual penetration test of the contractor network shall include any approved Internet infrastructure. Compliance with existing requirements to conduct quarterly vulnerability scans and annual 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:
        - CMS Technical Reference Architecture, Version 1.0, and all its appendices, and
        - CMS Java EE Application Development Guidelines.
    - 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 Integrated IT Investment & System Life Cycle Framework (Checkpoints, Deliverables, and Activities including *Security Authorization*) in introducing the new functionality.
    - Satisfactory systems test and evaluation of the Internet application to include evaluation of all 17 control categories set forth in the CMSRs.
    - 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; and NIST SP 800-115, Technical Guide to Information Security Testing and Assessment.

- *Security Authorization* dependent on compliance with security control requirements and completion of documentation such as the IS RA, the IS SSP for the infrastructure, platform, and applications supporting the Internet functionality, and a CP for the supporting platform and application. The IS RA 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.hhs.gov/InformationSecurity/14_Standards.asp#.

3. Privacy: Completion of a 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 CMSRs. An application for these uses is not required. If not already

emplaced, 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 *I*nternet for these purposes.

Appendix A:
Medicare Information Technology (IT) Systems Contingency Planning

References

(Rev.11, Issued: 09-30-11, Effective: 10-31-11, Implementation:10-31-11)

In addition to this manual, the following documents may be referenced during the IT systems contingency planning process:

- NIST Special Publication 800-34 *Rev. 1*, Contingency Planning Guide for Information Technology Systems, *May 2010*.
  http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1.pdf

- 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

- Health Insurance Portability & Accountability Act (HIPAA): The Race to Become Compliant, Ed Deveau, Disaster Recovery Journal, Fall 2000.

- Federal Information System Controls Audit Manual (FISCAM), Exposure Draft, GAO-08-1029G, Section 3.5.
  http://www.gao.gov/new.items/d081029g.pdf

- Presidential Decision Directive/NSC 63 (PDD 63), White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998.
  http://www.usdoj.gov/criminal/cybercrime/white_pr.htm

- OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004.
  http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html

- 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

- CMS Contingency Planning Tabletop Test Procedures, Version 1.1., 25 July 2007.
  http://www.cms.hhs.gov/informationsecurity/downloads/cp_tabletop_template.zip