



Chief Information Officer  
Office of Information Services  
Centers for Medicare & Medicaid Services

# **CMS POLICY FOR THE INFORMATION SECURITY PROGRAM**

December 31, 2008

Document Number: CMS-CIO-POL-SEC02-03.2

## Table of Contents

<b>1.</b>	<b>PURPOSE</b> .....	<b>1</b>
<b>2.</b>	<b>BACKGROUND</b> .....	<b>1</b>
<b>3.</b>	<b>SCOPE</b> .....	<b>5</b>
<b>4.</b>	<b>POLICY</b> .....	<b>5</b>
<b>4.1</b>	<b>ACCESS CONTROL (AC)</b> .....	<b>6</b>
4.1.1.	Access Control Policy and Procedures (AC-1) .....	6
4.1.2.	Account Management (AC-2) .....	6
4.1.3.	Access Enforcement (AC-3) .....	6
4.1.4.	Information Flow Enforcement (AC-4) .....	7
4.1.5.	Separation of Duties (AC-5).....	7
4.1.6.	Least Privilege (AC-6) .....	7
4.1.7.	Unsuccessful Log-On Attempts (AC-7).....	7
4.1.8.	System Use Notification (AC-8) .....	7
4.1.9.	Previous Log-On Notification (AC-9) .....	8
4.1.10.	Concurrent Session Control (AC-10).....	8
4.1.11.	Session Lock (AC-11).....	8
4.1.12.	Session Termination (AC-12) .....	8
4.1.13.	Supervision and Review—Access Control (AC-13).....	8
4.1.14.	Permitted Actions without Identification or Authentication (AC-14).....	8
4.1.15.	Automated Marking (AC-15).....	9
4.1.16.	Automated Labeling (AC-16) .....	9
4.1.17.	Remote Access (AC-17).....	9
4.1.18.	Wireless Access Restrictions (AC-18).....	9
4.1.19.	Access Control for Portable and Mobile Devices (AC-19).....	9
4.1.20.	Use of External Information Systems (AC-20).....	10
4.1.21.	System Boot Access (AC-CMS-1).....	10
<b>4.2</b>	<b>AWARENESS AND TRAINING (AT)</b> .....	<b>10</b>
4.2.1	Security Awareness and Training Policy and Procedures (AT-1) .....	10
4.2.2	Security Awareness (AT-2).....	11
4.2.3	Security Training (AT-3).....	11
4.2.4	Security Training Records (AT-4) .....	11
4.2.5	Contacts with Security Groups and Associations (AT-5) .....	11
<b>4.3</b>	<b>AUDIT AND ACCOUNTABILITY (AU)</b> .....	<b>11</b>
4.3.1.	Audit and Accountability Policy and Procedures (AU-1).....	11
4.3.2.	Auditable Events (AU-2).....	11
4.3.3.	Content of Audit Records (AU-3).....	12
4.3.4.	Audit Storage Capacity (AU-4).....	12
4.3.5.	Response to Audit Processing Failures (AU-5) .....	12
4.3.6.	Audit Monitoring, Analysis, and Reporting (AU-6) .....	12
4.3.7.	Audit Reduction and Report Generation (AU-7) .....	12
4.3.8.	Time Stamps (AU-8).....	12
4.3.9.	Protection of Audit Information (AU-9) .....	12
4.3.10.	Non-Repudiation (AU-10) .....	13
4.3.11.	Audit Record Retention (AU-11).....	13

<b>4.4</b>	<b>CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS (CA)</b> .....	<b>13</b>
4.4.1.	Certification, Accreditation, and Security Assessments Policies and Procedures ..... (CA-1) .....	13
4.4.2.	Security Assessments (CA-2).....	14
4.4.3.	Information System Connections (CA-3).....	14
4.4.4.	Security Certification (CA-4).....	14
4.4.5.	Plan of Action and Milestones (POA&M) (CA-5) .....	14
4.4.6.	Security Accreditation (CA-6) .....	15
4.4.7.	Continuous Monitoring (CA-7).....	15
<b>4.5</b>	<b>CONFIGURATION MANAGEMENT (CM)</b> .....	<b>15</b>
4.5.1.	Configuration Management Policy and Procedures (CM-1).....	15
4.5.2.	Baseline Configuration (CM-2).....	16
4.5.3.	Configuration Change Control (CM-3).....	16
4.5.4.	Monitoring Configuration Changes (CM-4) .....	16
4.5.5.	Access Restrictions for Change (CM-5) .....	16
4.5.6.	Configuration Settings (CM-6) .....	16
4.5.7.	Least Functionality (CM-7).....	17
4.5.8.	Information System Component Inventory (CM-8).....	17
<b>4.6</b>	<b>CONTINGENCY PLANNING (CP)</b> .....	<b>17</b>
4.6.1.	Contingency Planning Policy and Procedures (CP-1).....	17
4.6.2.	Contingency Plan (CP-2).....	17
4.6.3.	Contingency Training (CP-3).....	17
4.6.4.	Contingency Plan Testing and Exercises (CP-4) .....	18
4.6.5.	Contingency Plan Update (CP-5) .....	18
4.6.6.	Alternate Storage Site (CP-6).....	18
4.6.7.	Alternate Processing Site (CP-7).....	18
4.6.8.	Telecommunications Services (CP-8).....	18
4.6.9.	Information System Backup (CP-9).....	18
4.6.10.	Information System Recovery and Reconstitution (CP-10).....	19
<b>4.7</b>	<b>IDENTIFICATION AND AUTHENTICATION (IA)</b> .....	<b>19</b>
4.7.1.	Identification and Authentication Policy and Procedures (IA-1).....	19
4.7.2.	User Identification and Authentication (IA-2) .....	19
4.7.3.	Device Identification and Authentication (IA-3) .....	19
4.7.4.	Identifier Management (IA-4).....	19
4.7.5.	Authenticator Management (IA-5).....	20
4.7.6.	Authenticator Feedback (IA-6) .....	20
4.7.7.	Cryptographic Module Authentication (IA-7) .....	21
<b>4.8</b>	<b>INCIDENT RESPONSE (IR)</b> .....	<b>21</b>
4.8.1.	Incident Response Policy and Procedures (IR-1).....	21
4.8.2.	Incident Response Training (IR-2).....	21
4.8.3.	Incident Response Testing and Exercises (IR-3) .....	21
4.8.4.	Incident Handling (IR-4).....	21
4.8.5.	Incident Monitoring (IR-5).....	21
4.8.6.	Incident Reporting (IR-6).....	22
4.8.7.	Incident Response Assistance (IR-7) .....	22

**4.9 MAINTENANCE (MA) ..... 22**

4.9.1. System Maintenance Policy and Procedures (MA-1) ..... 22

4.9.2. Controlled Maintenance (MA-2)..... 22

4.9.3. Maintenance Tools (MA-3)..... 23

4.9.4. Remote Maintenance (MA-4) ..... 23

4.9.5. Maintenance Personnel (MA-5) ..... 23

4.9.6. Timely Maintenance (MA-6) ..... 23

4.9.7. Off-site Physical Repair of Systems (MA-CMS-1) ..... 23

4.9.8. On-site Physical Repair of Systems (MA-CMS-2) ..... 23

**4.10 MEDIA PROTECTION (MP)..... 23**

4.10.1. Media Protection Policy and Procedures (MP-1)..... 23

4.10.2. Media Access (MP-2)..... 24

4.10.3. Media Labeling (MP-3)..... 24

4.10.4. Media Storage (MP-4)..... 24

4.10.5. Media Transport (MP-5) ..... 24

4.10.6. Media Sanitization and Disposal (MP-6) ..... 24

4.10.7. Media Related Records (MP-CMS-1)..... 25

**4.11 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)..... 25**

4.11.1. Physical and Environmental Protection Policy and Procedures (PE-1) ..... 25

4.11.2. Physical Access Authorizations (PE-2)..... 25

4.11.3. Physical Access Control (PE-3) ..... 25

4.11.4. Access Control for Transmission Medium (PE-4) ..... 26

4.11.5. Access Control for Display Medium (PE-5) ..... 26

4.11.6. Monitoring Physical Access (PE-6) ..... 26

4.11.7. Visitor Control (PE-7)..... 26

4.11.8. Access Records (PE-8)..... 26

4.11.9. Power Equipment and Power Cabling (PE-9)..... 27

4.11.10. Emergency Shutoff (PE-10) ..... 27

4.11.11. Emergency Power (PE-11)..... 27

4.11.12. Emergency Lighting (PE-12) ..... 27

4.11.13. Fire Protection (PE-13) ..... 27

4.11.14. Temperature and Humidity Controls (PE-14)..... 27

4.11.15. Water Damage Protection (PE-15)..... 28

4.11.16. Delivery and Removal (PE-16) ..... 28

4.11.17. Alternate Work Site (PE-17) ..... 28

4.11.18. Location of Information System Components (PE-18)..... 28

4.11.19. Information Leakage (PE-19)..... 28

**4.12 PLANNING (PL)..... 28**

4.12.1. Security Planning Policy and Procedures (PL-1) ..... 28

4.12.2. System Security Plan (SSP) (PL-2)..... 29

4.12.3. System Security Plan Update (PL-3)..... 29

4.12.4. Rules of Behavior (ROB) (PL-4) ..... 29

4.12.5. Privacy Impact Assessment (PIA) (PL-5)..... 30

4.12.6. Security-Related Activity Planning (PL-6) ..... 30

**4.13 PERSONNEL SECURITY (PS)..... 31**

4.13.1. Personnel Security Policy and Procedures (PS-1)..... 31

4.13.2.	Position Categorization (PS-2).....	31
4.13.3.	Personnel Screening (PS-3).....	31
4.13.4.	Personnel Termination (PS-4).....	31
4.13.5.	Personnel Transfer (PS-5).....	32
4.13.6.	Access Agreements (PS-6).....	32
4.13.7.	Third-Party Personnel Security (PS-7).....	32
4.13.8.	Personnel Sanctions (PS-8).....	32
4.13.9.	Review System Access during Extraordinary Personnel Circumstances (PS-CMS-1) .....	32
4.13.10.	Designate an Information System Security Officer (ISSO) / System Security Officer (SSO) (PS-CMS-2).....	33
<b>4.14</b>	<b>RISK ASSESSMENT (RA).....</b>	<b>33</b>
4.14.1.	Risk Assessment Policy and Procedures (RA-1) .....	33
4.14.2.	Security Categorization (RA-2).....	33
4.14.3.	Risk Assessment (RA-3) .....	33
4.14.4.	Risk Assessment Update (RA-4).....	34
4.14.5.	Vulnerability Scanning (RA-5) .....	34
<b>4.15</b>	<b>SYSTEM AND SERVICES ACQUISITION (SA).....</b>	<b>34</b>
4.15.1.	System and Services Acquisition Policy and Procedures (SA-1) .....	34
4.15.2.	Allocation of Resources (SA-2) .....	34
4.15.3.	Life Cycle Support (SA-3) .....	34
4.15.4.	Acquisitions (SA-4).....	35
4.15.5.	Information System Documentation (SA-5) .....	35
4.15.6.	Software Usage Restrictions (SA-6) .....	36
4.15.7.	User Installed Software (SA-7) .....	36
4.15.8.	Security Engineering Principles (SA-8).....	36
4.15.9.	External Information System Services (SA-9).....	36
4.15.10.	Developer Configuration Management (SA-10).....	36
4.15.11.	Developer Security Testing (SA-11).....	36
<b>4.16</b>	<b>SYSTEM AND COMMUNICATIONS PROTECTION (SC).....</b>	<b>37</b>
4.16.1.	System and Communications Protection Policy and Procedures (SC-1).....	37
4.16.2.	Application Partitioning (SC-2) .....	37
4.16.3.	Security Function Isolation (SC-3).....	37
4.16.4.	Information Remnance (SC-4).....	37
4.16.5.	Denial of Service Protection (SC-5).....	37
4.16.6.	Resource Priority (SC-6).....	37
4.16.7.	Boundary Protection (SC-7).....	38
4.16.8.	Transmission Integrity (SC-8).....	38
4.16.9.	Transmission Confidentiality (SC-9) .....	38
4.16.10.	Network Disconnect (SC-10) .....	38
4.16.11.	Trusted Path (SC-11).....	38
4.16.12.	Cryptographic Key Establishment and Management (SC-12).....	38
4.16.13.	Use of Cryptography (SC-13) .....	39
4.16.14.	Public Access Protections (SC-14).....	39
4.16.15.	Collaborative Computing (SC-15) .....	39
4.16.16.	Transmission of Security Parameters (SC-16) .....	39

4.16.17. Public Key Infrastructure Certificates (SC-17) ..... 39

4.16.18. Mobile Code (SC-18) ..... 39

4.16.19. Voice Over Internet Protocol (SC-19)..... 39

4.16.20. Secure Name / Address Resolution Service (Authoritative Source) (SC-20) ..... 40

4.16.21. Secure Name / Address Resolution Service (Recursive or Caching Resolver) (SC-21) ..... 40

4.16.22. Architecture and Provisioning for Name / Address Resolution Service (SC-22) ..... 40

4.16.23. Session Authenticity (SC-23)..... 40

4.16.24. Desktop Modems (SC-CMS-1) ..... 40

4.16.25. Identify and Detect Unauthorized Modems (SC-CMS-2)..... 40

4.16.26. Secondary Authentication and Encryption (SC-CMS-3) ..... 40

4.16.27. Electronic Mail (SC-CMS-4) ..... 40

4.16.28. Persistent Cookies (SC-CMS-5)..... 41

4.16.29. Network Interconnection (SC-CMS-6) ..... 41

**4.17 SYSTEM AND INFORMATION INTEGRITY (SI) ..... 41**

4.17.1. System and Information Integrity Policy and Procedures (SI-1) ..... 41

4.17.2. Flaw Remediation (SI-2)..... 41

4.17.3. Malicious Code Protection (SI-3)..... 41

4.17.4. Information System Monitoring Tools and Techniques (SI-4) ..... 41

4.17.5. Security Alerts and Advisories (SI-5) ..... 42

4.17.6. Security Functionality Verification (SI-6) ..... 42

4.17.7. Software and Information Integrity (SI-7) ..... 42

4.17.8. Spam Protection (SI-8)..... 42

4.17.9. Information Input Restrictions (SI-9)..... 42

4.17.10. Information Accuracy, Completeness, Validity, and Authenticity (SI-10)..... 42

4.17.11. Error Handling (SI-11) ..... 42

4.17.12. Information Output Handling and Retention (SI-12)..... 43

**5. ROLES AND RESPONSIBILITIES ..... 43**

**5.1 CMS ADMINISTRATOR..... 43**

**5.2 CMS CHIEF INFORMATION OFFICER (CIO)..... 43**

**5.3 CHIEF INFORMATION SECURITY OFFICER (CISO)..... 44**

**5.4 COMPONENT ISSOS ..... 44**

**5.5 BUSINESS OWNERS ..... 45**

**5.6 SYSTEM ADMINISTRATORS ..... 45**

**5.7 SYSTEM DEVELOPERS / MAINTAINERS..... 45**

**5.8 CMS / BUSINESS PARTNER / CONTRACTOR EMPLOYEES ..... 45**

**5.9 USERS..... 46**

**6. APPLICABLE LAWS/GUIDANCE ..... 46**

**7. INFORMATION AND ASSISTANCE ..... 47**

**8. EFFECTIVE DATE/IMPLEMENTATION ..... 47**

**9. APPROVED ..... 47**

**10. ASSOCIATED RESOURCES ..... 48**

**GLOSSARY..... 48**

## Figures and Tables

Figure 1: CMS IS Program Risk Management Process.....	4
Table 1: NIST SP 800-53 IS Control Families and Classes .....	5

## Nature of Changes

**Version SEC02-03.2:** This is a revision to the June 25, 2008 issuance of the *CMS Policy for the Information Security Program* in response to providing the CIO or his/her designated representative authority in accordance with Department policy to approve alternate mitigations when encryption of desktops is not feasible and physical controls and other management controls are in place. Also the Scope was enhanced to include that this policy applies to business partners and sub-contractors “doing work on behalf of CMS”. All changes, other than modifications to Section 4.1.3 and Scope, are editorial in nature. The changes to this policy can be found in the following sections:

1. Section 1, Purpose, has been modified to update the statement that this version of the policy supersedes the previous version dated June 25, 2008.
2. Section 2, Background, has been modified to update the NIST SP 800-53 version to NIST SP 800-53 Rev. 2 to indicate the current version.
3. Section 3, Scope, has been modified to state that this policy also applies to Business Partners and sub-contractors “doing work on behalf of CMS.”
4. Section 4, Policy, has been modified to update the NIST SP 800-53 version to NIST SP 800-53 Rev. 2 to indicate the current version.
  - a. Section 4.1.3, last sentence, has been modified to require CIO or designate approval to employ alternate controls.
  - b. Section 4.4.4, has been modified to capitalize “Business Owners” for document consistency.
  - c. Section 4.17.3, has been modified to capitalize “Business Owners” for document consistency.
5. Section 6, Applicable Laws/Guidance, has been modified to include “Change Notice 2” to the FIPS 140-2 reference to clarify the reference date. The NIST SP 800-53 reference has been modified to NIST SP 800-53 Rev.2 with a date of December 2007 to reflect the current version.
6. Section 10, Associated Resources, removed trailing “/” from the CMS CIO Directives hyperlink.
7. Glossary, All Glossary references to NIST SP 800-53R1 have been modified to NIST SP 800-53R2 to reflect the current version. All Glossary references to NIST SP 800-53 have been modified to NIST SP 800-53R2 to reflect the current version.

**Version SEC02-03.1:** This is a revision to the April 24, 2008 issuance of the *CMS Policy for the Information Security Program*, in response to CMS modifying this policy to comply with the HHS Chief of Staff memo on *Mandatory Protection of Sensitive Information on Computers*,

*Mobile Devices and Portable Media*, dated May 19, 2008. Modifications can be found in the following sections:

1. Section 1, Purpose, has been modified to add a statement that this version of the policy supersedes the previous version dated April 24, 2008.
2. Section 4, Policy, has been modified as follows:
  - a. Section 4.1.3 Access Enforcement (AC-3) was modified to add “In addition, encryption as access enforcement extends to all government and non-government furnished desktop computers that store sensitive information. While encryption is the preferred technical solution for protection of sensitive information on all desktop computers, adequate physical security controls and other management controls are acceptable mitigations for the protection of desktop computers.” to include the desktop encryption requirement.
  - b. Section 4.12.4 Rules of Behavior (PL-4) was changed from “ROBs shall be established and made readily available...” to “ROBs shall be established in alignment with HHS requirements <http://hhs.gov/ocio/policy/2008-0001.003s.html>, and made readily available...” to meet the requirement that all CMS employees and contractors review and sign the HHS ROB.

**Version SEC02-03:** This is a revision to the November 15, 2007 issuance of the *CMS Policy for the Information Security Program*, in response to CMS modifying this policy and the *CMS Information Security Acceptable Risk Safeguards (ARS)* to align the CMS organizationally defined variables to the current CMS processes. Modifications to this policy can be found in the following sections:

1. Section 1, Purpose, has been modified to add a statement that this version of the policy supersedes the previous version dated November 15, 2007.
2. Section 4, Policy, has been modified to correct an inaccuracy in the November 15, 2007 issuance of this policy and to apply a global change to replace the terms “annually” or “annual” with “every 365 days”. Section 4.6.6 which originally stated “Agreements with an alternate processing site shall...” should read “Agreements with an alternate storage site...” Section 4.12.4 originally stated “Before authorizing access to the information system and its resident information...”) and has been changed to “Before authorizing access to the information system and / or information and annually thereafter ...” to cover access to information even if no access to a CMS information system.

---

## 1. PURPOSE

This document establishes the policy for the information security (IS) program at the Centers for Medicare & Medicaid Services (CMS). The formation of the CMS IS Program Policy is driven by many factors, the key one being **Risk**. This policy sets the ground rules under which CMS shall operate and safeguard its information and information systems to reduce the risk, and minimize the effect of security incidents.

This policy supersedes the previous version that was signed by the CMS Chief Information Officer (CIO) on June 25, 2008.

---

## 2. BACKGROUND

As the Agency charged with administering the Medicare, Medicaid, and State Children's Health Insurance Programs, CMS collects, generates, and stores financial, health care, and other sensitive information. Most of this information relates to the health care provided to the nation's Medicare and Medicaid beneficiaries and has access restrictions required by legislative and regulatory directives. As the information's trusted custodian, CMS must protect and ensure the confidentiality, integrity, and availability (CIA) of all its information regardless of how it is created, distributed, or stored.

To safeguard the CIA of its information and information systems effectively, CMS has established an enterprise-wide IS Program. As part of this program, security controls must be implemented to protect all information assets, including hardware, systems, software, and data. These controls must be designed to ensure compliance with all federal legislation, policies and standards (e.g., by managing risk; facilitating change control; reporting and responding to security incidents, intrusions, or violations; and formulating contracts).

This policy addresses the reduction in risks to information resources through adoption of preventive measures and controls designed to detect any errors that occur. It also addresses the recovery of information resources in the event of a disaster. For ease of use, this policy is organized into **classes and families**. CMS has established three (3) classes of IS controls: Management, Operational, and Technical. This structure is consistent with the guidance established by the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53, Rev. 2, *Recommended Security Controls for Federal Information Systems*.

**Management** controls involve those safeguards and countermeasures that manage the security of the information and information systems, and the associated risk to CMS' assets and operations. There are four (4) families of policy within the Management class that address:

1. Certification, Accreditation, and Security Assessments (CA);
2. Planning (PL);
3. Risk Assessment (RA); and
4. System and Services Acquisition (SA).

**Operational** controls support the day-to-day procedures and mechanisms to protect CMS' information and information systems. There are nine (9) families of policy within the Operational class that address:

1. Awareness and Training (AT);
2. Configuration Management (CM);
3. Contingency Planning (CP);
4. Incident Response (IR);
5. Maintenance (MA);
6. Media Protection (MP);
7. Physical and Environmental Protection (PE);
8. Personnel Security (PS); and
9. System and Information Integrity (SI).

**Technical** controls are those security mechanisms employed within an information system's hardware, software, or firmware to protect the system and its information from unauthorized access, use, disclosure, disruption, modification, or destruction. They are used to authorize or restrict the activities of all levels of users within an individual system by employing access based on a least-privileged and need-to-know approach. There are four (4) families of policy within the Technical class that address:

1. Access Control (AC);
2. Audit and Accountability (AU);
3. Identification and Authentication (IA); and
4. System and Communications Protection (SC).

## **IS Program Activities**

This section describes some of the key activities in an organizational IS program. These activities are conducted within the system developmental life-cycle. See Figure 1 below.

### ***Security Categorization***

Security categorization establishes three (3) impact levels (low, moderate, high) for each of the stated security objectives, i.e., CIA, relevant to securing information resource.

### ***Risk Assessment***

In accordance with the provisions of Federal Information Security Management Act (FISMA), IS programs are required to conduct a periodic assessment of risks, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization.

### ***Security Planning***

In accordance with the provisions of FISMA, IS programs are required to have plans for providing adequate IS for networks, facilities, information systems, or groups of information systems, as appropriate.

***Security Control Development***

The security controls, which are described in the security plans, shall be designed, developed, and implemented effectively. For information systems in operation, the development or integration of additional security controls or the modification of selected controls may be necessary.

***Developmental Security Test and Evaluation (ST&E)***

The security controls must be tested and evaluated prior to deployment to ensure that the controls are effective. An ST&E plan is developed to test the security controls. This plan guides the developmental security testing and evaluation of the security controls and provides feedback to Business Owners, developers, and integrators.

***Security Control Integration***

The integration of security controls occurs at the operational sites where the information systems are to be deployed for operations.

***Security Control Verification***

In accordance with the provisions of FISMA, periodic testing and evaluation of the security controls in an information system are required in order to ensure that the controls are implemented effectively. The comprehensive evaluation of security control effectiveness through established verification techniques and procedures, also known as security certification, is a critical activity conducted by the organization or by an independent third party on behalf of the organization.

***Security Authorization***

In accordance with the provisions of Office of Management and Budget (OMB) Circular A-130, a security authorization of an information system to process, store, or transmit information is required. This authorization, i.e., security accreditation granted by a senior organizational official, is based on the verified effectiveness of security controls to some agreed-upon-level of assurance together with an identified risk to the organization's operation or assets.

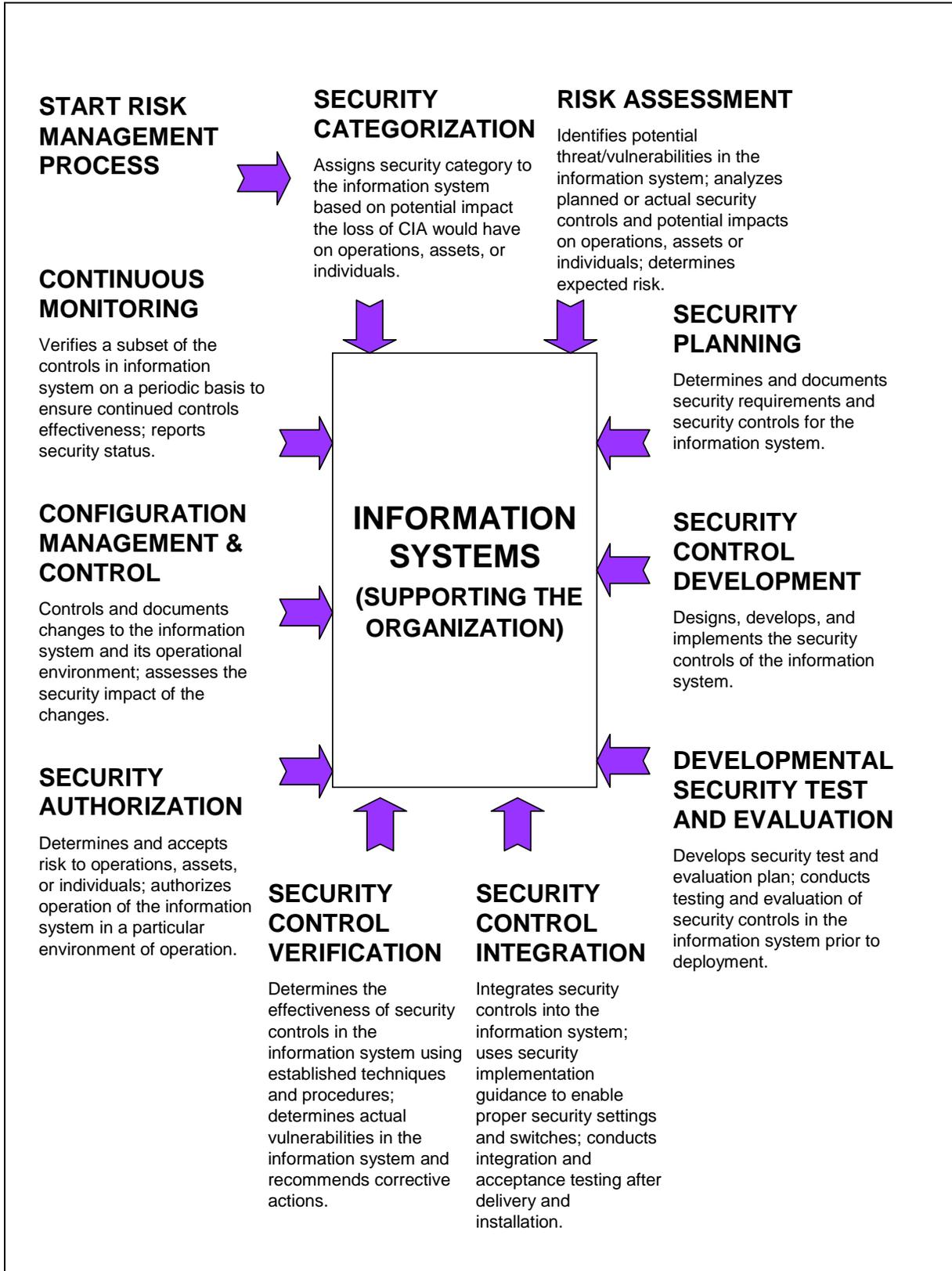
***Configuration and Management Control***

Changes to an information system can have a significant impact on the security of the system. Configuration management procedures are critical to the establishment of an initial baseline of hardware, software, and firmware components for an information system and the subsequent control and maintenance of an accurate inventory of changes to the system.

***On-going Monitoring***

In accordance with the provisions of FISMA, periodic testing and evaluation of security controls in an information system are required on an on-going basis to ensure that the controls continue to be effective in their application. The on-going monitoring of security control effectiveness can be accomplished in a variety of ways including security reviews, self-assessments, security testing and evaluation, or audits.

**Figure 1: CMS IS Program Risk Management Process**



### 3. SCOPE

This policy applies to all CMS information, information systems, IT activities, and IT assets owned, leased, controlled, or used by CMS, CMS’ agents, contractors, or other business partners on behalf of CMS. This policy applies to all CMS employees, contractors (including all Business Partners as defined in Section 1.0 of the Business Partners System Security Manual ([http://www.cms.hhs.gov/manuals/downloads/117\\_systems\\_security.pdf/](http://www.cms.hhs.gov/manuals/downloads/117_systems_security.pdf/)), sub-contractors, and their respective facilities supporting CMS business missions, wherever CMS data is stored or processed. Some policies are explicitly stated for persons with a specific job function (e.g. the System Administrator); otherwise, all personnel supporting CMS business functions shall comply with the policies. CMS operating departments shall use this policy or may create a more restrictive policy, but not one that is less restrictive, less comprehensive, or less compliant than this policy.

This policy does not supersede any other applicable law or higher level agency directive, or existing labor management agreement in effect as of the effective date of this policy.

### 4. POLICY

CMS’ policies and controls have a well-defined organization and structure. Security policies and controls are organized into classes and families for ease of use in the control selection and specification process. There are three (3) general classes of security policies and controls (i.e., Management, Operational, and Technical) and seventeen (17) security policy and control families as specified in NIST SP 800-53, Rev 2.

Each family contains security policies and controls related to the security functionality of the family. A two character identifier is assigned to uniquely identify each policy and control family. The following table summarizes the classes and families in the security control catalog and the associated family identifiers, as well as the order of the included policies.

**Table 1: NIST SP 800-53 IS Control Families and Classes**

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational

Identifier	Family	Class
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

## 4.1 Access Control (AC)

### 4.1.1. Access Control Policy and Procedures (AC-1)

Logical access controls and procedures shall be established and implemented effectively to ensure that only designated individuals, under specified conditions (e.g. time of day, port of entry, type of authentication) can access the CMS information system, activate specific commands, execute specific programs and procedures, or create views or modify specific objects (i.e., programs, information, system parameter). Procedures shall be developed to guide the implementation and management of logical access controls. The logical access controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, and shall be periodically reviewed, and, if necessary, updated.

### 4.1.2. Account Management (AC-2)

Comprehensive account management mechanisms shall be established to: identify account types (i.e., individual, group, and system); establish conditions for group membership; and assign associated authorizations. Access to the CMS information system shall be granted based on: (a) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (b) intended system usage. Proper identification and approval shall be required for requests to establish information system accounts.

Account control mechanisms shall be in place and supporting procedures shall be developed, documented and implemented effectively to authorize and monitor the use of guest / anonymous accounts; and to remove, disable, or otherwise secure unnecessary accounts. Account managers shall be notified when CMS information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers shall also be notified when users' information system usage or need-to-know changes.

### 4.1.3. Access Enforcement (AC-3)

Access enforcement mechanisms shall be developed, documented and implemented effectively to control access between named users (or processes) and named objects (e.g., files and programs) in a CMS information system. Additional application level access enforcement mechanism shall be implemented, when necessary, to provide increased

information security for CMS information. When encryption of stored information is employed as an access enforcement mechanism, it shall be encrypted using validated cryptographic modules (see section 4.16.13).

In addition, encryption as access enforcement extends to all government and non-government furnished desktop computers that store sensitive information. While encryption is the preferred technical solution for protection of sensitive information on all desktop computers, adequate physical security controls and other management controls are acceptable mitigations for the protection of desktop computers with the approval of the CIO or his/her designated representative.

#### 4.1.4. Information Flow Enforcement (AC-4)

Flow control shall be enforced over information between source and destination objects within CMS information systems and between interconnected systems based on the characteristics of the information.

#### 4.1.5. Separation of Duties (AC-5)

The principle of separation of duties shall be enforced to eliminate conflicts of interest in the responsibilities and duties assigned to individuals. Mission functions and distinct information systems support functions shall be divided among different roles, and support functions shall be performed by different individuals (e.g., personnel responsible for administering access control functions shall not also administer audit functions). Personnel developing and testing system code shall not have access to production libraries. Access control software shall be in place to limit individual authority and information access, such that the collusion of two or more individuals is required to commit fraudulent activity. Job descriptions shall reflect accurately the assigned duties and responsibilities that support separation of duties.

#### 4.1.6. Least Privilege (AC-6)

Each user or process shall be assigned the most restrictive set of privileges needed for the performance of authorized tasks.

#### 4.1.7. Unsuccessful Log-On Attempts (AC-7)

Automated mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enforce a limit of CMS-defined consecutive invalid access attempts by a user during a specified time period. Systems shall be locked after a specified number of multiple unsuccessful log-on attempts.

#### 4.1.8. System Use Notification (AC-8)

An approved warning / notification message shall be displayed upon successful log-on and before gaining system access. The warning message shall notify users that the CMS information system is owned by the U.S. Government and shall describe conditions for

access, acceptable use, and access limitations. The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies) and shall remain on the screen until the user takes explicit actions to log-on to the CMS information system.

#### 4.1.9. Previous Log-On Notification (AC-9)

Automated mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to provide users with information about previous log-ons, both successful and unsuccessful.

#### 4.1.10. Concurrent Session Control (AC-10)

Automated mechanisms shall be in place to limit the number of concurrent user sessions, based upon the established business needs of the user, CMS, and the sensitivity level of the CMS information system.

#### 4.1.11. Session Lock (AC-11)

Automated session lock mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable locking of the information system session by the user. The information system shall also detect inactivity and block further access until the user re-establishes the connection using proper identification and authentication processes.

#### 4.1.12. Session Termination (AC-12)

The information system shall identify and terminate all inactive remote sessions (both user and information system sessions) automatically.

#### 4.1.13. Supervision and Review—Access Control (AC-13)

Personnel shall be supervised and reviewed with respect to the usage of CMS information system access controls. Automated mechanisms shall be in place to facilitate the review of audit records, and any unusual activities shall be investigated in a timely manner. Changes to access authorizations shall be reviewed periodically. The activities of users with significant information system roles and responsibilities shall be reviewed more frequently.

#### 4.1.14. Permitted Actions without Identification or Authentication (AC-14)

Based upon mission / business requirements, public access to CMS information systems without identification and authorization shall be limited to public websites and other publicly available systems. CMS information systems shall be configured to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.

#### 4.1.15. Automated Marking (AC-15)

Automated mechanisms shall be in place to mark CMS information system output using standard naming convention, in order to identify any special dissemination, handling, or distribution instructions.

#### 4.1.16. Automated Labeling (AC-16)

CMS information systems shall label information “in storage,” “in process,” and “in transit” with special dissemination handling or distribution instructions, in a manner consistent with this policy.

#### 4.1.17. Remote Access (AC-17)

Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can access the information system from remote locations shall be limited and justification / approval for such access shall be controlled, documented, and monitored.

Dial-up lines, other than those with FIPS 140 (as amended) validated cryptography, shall not be used to gain access to a CMS information system that processes CMS sensitive information unless the CIO or his/her designated representative, provides specific written authorization. Periodic monitoring shall be implemented to ensure that installed equipment does not include unanticipated dial-up capabilities.

#### 4.1.18. Wireless Access Restrictions (AC-18)

Installation of wireless access points (WAP) into CMS information systems and networks shall be prohibited unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. Authorized WAP devices and wireless access shall be monitored on a regular basis, and wireless communications shall be secured through the use of approved encryption controls.

#### 4.1.19. Access Control for Portable and Mobile Devices (AC-19)

The connection of portable and mobile devices (e.g., notebook computers, personal digital assistants (PDA), cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to CMS information systems and networks shall be prohibited unless explicitly authorized, in writing, by the CIO or his/her designated representative. Prior to connecting portable and mobile devices to CMS information systems and networks, such devices shall be configured to comply with CMS IS policies and procedures. The storage and transmission of CMS sensitive information on portable and mobile information devices shall be protected with activities such as scanning the devices for malicious code, virus protection software, and disabling unnecessary hardware. The activities and controls shall be commensurate with the system security level of the information.

#### 4.1.20. Use of External Information Systems (AC-20)

External information systems, including, but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports shall not be used to store, access, transmit, or process CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative.

Strict terms and conditions shall be established for the use of external information systems. The terms and conditions shall address, at a minimum:

- 4.1.20.1 The types of applications that can be accessed from external information systems;
- 4.1.20.2 The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
- 4.1.20.3 How other users of the external information system will be prevented from accessing federal information;
- 4.1.20.4 The use of virtual private networking (VPN) and firewall technologies;
- 4.1.20.5 The use of and protection against the vulnerabilities of wireless technologies;
- 4.1.20.6 The maintenance of adequate physical security controls;
- 4.1.20.7 The use of virus and spyware protection software; and
- 4.1.20.8 How often the security capabilities of installed software are to be updated.

#### 4.1.21. System Boot Access (AC-CMS-1)

System boot access shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can alter or perform non-standard boots of systems and/or components of the information system shall be limited and justification / approval for such access shall be controlled, documented, and monitored.

## 4.2 Awareness and Training (AT)

#### 4.2.1 Security Awareness and Training Policy and Procedures (AT-1)

An IS AT program shall be developed, documented, and implemented effectively for all personnel, including contractors and any other users of CMS information and information systems. The IS AT program shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-50. AT shall be completed by all personnel prior to granting authorization to access to CMS information, information systems, and networks.

#### 4.2.2 Security Awareness (AT-2)

Procedures shall be developed, documented, and implemented effectively to ensure that CMS information system users are aware of the system security requirements and their responsibilities toward enabling effective mission accomplishment. The IS AT program shall be consistent with 5 CFR Part 930 (<http://opm.gov/fedregis/2004/69-061404-32835-a.pdf>) and the guidance provided in NIST SP 800-50.

#### 4.2.3 Security Training (AT-3)

The organization shall identify and document all positions and/or roles with significant information system security responsibilities during the system development life cycle. All personnel with significant information system security responsibilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. Content of the security awareness training shall be determined based upon the information systems to which personnel have authorized access. The employee shall acknowledge having received the security and awareness training either in writing or electronically as part of the training course completion.

#### 4.2.4 Security Training Records (AT-4)

Procedures shall be developed, documented, and implemented effectively to ensure that individual IS training activities, including basic security awareness training and specific information system security training, are properly documented and monitored.

#### 4.2.5 Contacts with Security Groups and Associations (AT-5)

Contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations shall be encouraged and supported to enable security personnel to stay up to date with the latest recommended security practices, techniques, and technologies; and to share the latest security-related information including threats, vulnerabilities, and incidents.

### **4.3 Audit and Accountability (AU)**

#### 4.3.1. Audit and Accountability Policy and Procedures (AU-1)

All CMS information systems shall be configured to produce, store, and retain audit records of specific system, application, network, and user activity. Procedures shall be developed to guide the implementation and management of audit controls, and shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

#### 4.3.2. Auditable Events (AU-2)

Automated mechanisms shall be established which enable the ability to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact investigations of security incidents. The selection of auditable events shall be based upon a risk assessment

as to which events require auditing on a continuous basis, and which events require auditing in response to specific situations.

#### 4.3.3. Content of Audit Records (AU-3)

Automated mechanisms shall be established to provide the capability to include specific information in audit records. Audit records shall contain sufficient information to establish what events occurred, when the events occurred, the source of the events, the cause of the events, and the event outcome.

#### 4.3.4. Audit Storage Capacity (AU-4)

A sufficient amount of information system storage capacity shall be allocated for audit records, and information systems shall be configured to reduce the likelihood of audit records exceeding such storage capacity.

#### 4.3.5. Response to Audit Processing Failures (AU-5)

Automated mechanisms shall be established which provide the capability to generate information system alerts for appropriate officials in the event of an audit failure or audit storage capacity being reached and to take appropriate additional actions.

#### 4.3.6. Audit Monitoring, Analysis, and Reporting (AU-6)

Information system audit records shall be reviewed and analyzed regularly to identify and detect unauthorized, inappropriate, unusual, and/or suspicious activity. Such activity shall be investigated and reported to appropriate officials, in accordance with current CMS Procedures.

#### 4.3.7. Audit Reduction and Report Generation (AU-7)

Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to enable human review of audit information and the generation of appropriate audit reports.

#### 4.3.8. Time Stamps (AU-8)

Audit records shall employ time stamps for use in audit record generation. Time stamps of audit records shall be generated using internal system clocks that are synchronized system-wide.

#### 4.3.9. Protection of Audit Information (AU-9)

Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.

#### 4.3.10. Non-Repudiation (AU-10)

Non-repudiation mechanisms shall be implemented that enable a later determination whether a given individual sent a specific message and whether a given individual received a specific message.

#### 4.3.11. Audit Record Retention (AU-11)

Audit records shall be retained to provide support for after-the-fact investigations of security incidents, and to meet regulatory and/or CMS information retention requirements. The National Archives and Records Administration maintains criteria for record retention across many disciplines and information security retention standards shall not be construed to relieve or waive these other standards.

### 4.4 Certification, Accreditation, and Security Assessments (CA)

#### 4.4.1. Certification, Accreditation, and Security Assessments Policies and Procedures (CA-1)

All General Support Systems (GSSs) (i.e., hardware and related infrastructure) and Major Applications (MAs) (i.e., application code) shall be certified by the Business Owner and accredited by the CMS CIO or his/her designated representative to ensure that the security controls for each GSS or MA mitigate risk to an acceptable level for protecting the confidentiality, integrity, and availability (CIA) of CMS information and information systems. All C&A and security assessment activities shall be conducted in accordance with current CMS Procedures.

Unless there are major changes to a system, re-certification and re-accreditation of GSSs, MAs, and application systems shall be performed every three (3) years. If there are major changes to the GSS, MA, or application system, re-certification and re-accreditation shall be performed whenever the changes occur. Also, re-accreditation and/or re-certification shall be performed upon the completion of the certification / accreditation action lists, in the case of an interim accreditation. Further, the requirements for re-accreditation / re-certification are listed in section 4.4.6, Security Accreditation (CA-6).

If the CMS CIO or his/her designee is not satisfied that the system is protected at an acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls. Interim approval shall be granted only by the CMS CIO or his/her designated representative in lieu of a full denial to process. Interim approval to operate is not a waiver of the requirement for management approval to process. The information system shall meet all requirements and receive management approval to process by the interim approval expiration date. No extensions of interim accreditation shall be granted except by the CMS CIO or his/her designated representative.

As part of the system certification and accreditation (C&A), an independent evaluation based on the system security level may be performed and the results analyzed. Considering the evaluation results from the system testing, IS Risk Assessment (RA), System Security Plan (SSP), independent system tests and evaluations, the Business Owner and System Developer / Maintainer shall certify that the system meets the security requirements to the extent

necessary to protect CMS information adequately and meets an acceptable level of risk. Final accreditation shall be made by the CMS CIO or his/her designated representative.

#### 4.4.2. Security Assessments (CA-2)

Routine assessments of all CMS information systems shall be conducted prior to initial operational capability and authorization to operate; prior to each re-authorization to operate; or when a significant change to the information system occurs. Routine assessments of all CMS information systems shall determine if security controls are implemented correctly, are effective in their application, and comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Routine assessments shall be conducted every 365 days, in accordance with NIST SP 800-53 or an acceptable alternative methodology, to monitor the effectiveness of security controls. Findings are subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

#### 4.4.3. Information System Connections (CA-3)

Management shall authorize in writing through the use of system connection agreements all connections to other information systems outside of the accreditation boundary including systems owned and operated by another program, organization, or contractor in compliance with established CMS connection rules and approval processes. The system connections, which are connections between infrastructure components of a system or application, shall be monitored / controlled on an on-going basis.

#### 4.4.4. Security Certification (CA-4)

Business Owners shall conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The security certification process shall be integrated into and span across the SDLC. In addition, the Business Owner shall review the certification documentation every 365 days, update the documentation where necessary to reflect any changes to the system, and submit a copy of the updated information to the CIO or his/her designated representative.

#### 4.4.5. Plan of Action and Milestones (POA&M) (CA-5)

A POA&M shall be developed, implemented, and updated based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The POA&M shall document the planned, implemented, and evaluated corrective actions to repair deficiencies discovered during the security control assessment, and to reduce or eliminate any known vulnerability in the information system.

Personnel shall be designated to assign, track, and update risk mitigation efforts. Designated personnel shall define and authorize corrective action plans, and monitor corrective action progress.

#### 4.4.6. Security Accreditation (CA-6)

Explicit authorization to operate the information system shall be received from the CMS CIO or his/her designated representative prior to the system being placed into operations. If the authorization is an interim approval to operate, then the authorization shall be granted based on the designated security category of the information system. An explicit corrective action plan shall be developed, implemented effectively, and monitored by the authorizing official. Re-authorization shall be obtained prior to continued operation:

- 4.4.6.1 At least every three (3) years;
- 4.4.6.2 When substantial changes are made to the system;
- 4.4.6.3 When changes in requirements result in the need to process data of a higher sensitivity;
- 4.4.6.4 When changes occur to authorizing legislation or federal requirements;
- 4.4.6.5 After the occurrence of a serious security violation which raises questions about the validity of an earlier certification; and
- 4.4.6.6 Prior to expiration of a previous accreditation.

#### 4.4.7. Continuous Monitoring (CA-7)

Security controls in CMS information systems shall be monitored on an on-going basis. Selection criteria for control monitoring shall be established and a subset of the security controls employed within information systems shall be selected for continuous monitoring purposes.

## 4.5 Configuration Management (CM)

### 4.5.1. Configuration Management Policy and Procedures (CM-1)

A CM process that includes the approval, testing, implementation, and documentation of changes shall be developed, documented, and implemented effectively to track and control the hardware, software, and firmware components that comprise the CMS information system. The CM process shall be consistent with the organization's information technology architecture plans. Formally documented CM roles, responsibilities, procedures, and documentation shall be in place.

#### 4.5.2. Baseline Configuration (CM-2)

A baseline, operational configuration of the hardware, software, and firmware that comprise the CMS information system shall be developed and documented. Procedures shall be developed, documented, and implemented effectively to maintain the baseline configuration. The configuration of the information system shall be consistent with the Federal Enterprise Architecture and the organization's information system architecture.

#### 4.5.3. Configuration Change Control (CM-3)

Change control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to control changes to the information system. Change request forms shall be used to document requests with related approvals. Change requests shall be approved by the Business Owner, or his/her designated representative, and other appropriate organization officials including, but not limited to, the system maintainer and information system support staff.

Test plans shall be developed and approved for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, library control) and shall include appropriate consideration of security. Test results shall be documented and appropriate responsive actions shall be taken based on the results.

Emergency changes for the CMS information system shall be documented and approved by appropriate organization officials, either prior to the change or after the fact. Emergency changes to the configuration shall be documented appropriately and approved, and responsible personnel shall be notified for security analysis and follow-up.

#### 4.5.4. Monitoring Configuration Changes (CM-4)

Mechanisms to monitor change activity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to monitor information system changes and actions by privileged users. Security impact analyses shall be conducted after system changes are made to determine the IS-related effects of the changes. Activities associated with configuration changes to the information system shall be audited.

#### 4.5.5. Access Restrictions for Change (CM-5)

Access control change mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to approve individual access privileges and to enforce physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.

#### 4.5.6. Configuration Settings (CM-6)

Procedures shall be developed, documented, and implemented effectively to configure and benchmark information technology products in accordance with good security practice settings. Mandatory configuration settings for information technology products employed

within the information system shall be established. The security settings of information technology products shall be configured to the most restrictive mode consistent with information system operational requirements, documented, and enforced in all components of the information system.

#### 4.5.7. Least Functionality (CM-7)

Information systems shall be configured to provide only essential capabilities. The functions and services provided by CMS information systems shall be reviewed carefully to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol [VoIP], Instant Messaging [IM], File Transfer Protocol [FTP], Hyper Text Transfer Protocol [HTTP], file sharing). The use of those functions, ports, protocols, and/or services shall be prohibited and/or restricted.

#### 4.5.8. Information System Component Inventory (CM-8)

Procedures shall be developed, documented, and implemented effectively to document and maintain a current inventory of the information system's constituent components and relevant ownership information. The inventory of information system components shall include manufacturer, model / type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership.

## 4.6 Contingency Planning (CP)

### 4.6.1. Contingency Planning Policy and Procedures (CP-1)

All major CMS information systems shall be covered by a CP that complies with OMB Circular A-130 policy and is consistent with the intent of NIST SP 800-34. Documented procedures shall be developed to facilitate the implementation of the contingency planning policy and associated contingency planning controls. The contingency planning policy and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Contingency planning may result in manual processes in the instance of an actual event, instead of system recovery at an alternate site.

### 4.6.2. Contingency Plan (CP-2)

All major CMS information systems shall be covered by a CP, relative to the system security level, providing continuity of support in the event of a disruption of service. A CP for the information system shall address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. A CP for the information system shall be consistent with NIST SP 800-34. Designated officials within the organization shall review and approve the CP and distribute copies of the plan to key contingency personnel.

### 4.6.3. Contingency Training (CP-3)

Operational and support personnel (including managers and users of the information system) shall receive training in contingency operations and understand their contingency roles and

responsibilities with respect to the information system. Refresher training shall be provided to all contingency personnel.

#### 4.6.4. Contingency Plan Testing and Exercises (CP-4)

CPs shall be tested and/or exercised at least every 365 days using defined tests and exercises, such as the tabletop test in accordance with current CMS Procedures, to determine the plans' effectiveness and readiness to execute the plan. Test / exercise results shall be documented and reviewed by appropriate organization officials. Reasonable and appropriate corrective actions shall be initiated to close or reduce the impact of CP failures and deficiencies.

#### 4.6.5. Contingency Plan Update (CP-5)

CPs shall be reviewed at least every 365 days and, if necessary, revised to address system / organizational changes and/or any problems encountered during plan implementation, execution, or testing.

#### 4.6.6. Alternate Storage Site (CP-6)

Agreements with an alternate storage site shall be established and implemented effectively to permit the storage of CMS information system backup information. Copies of the current CP shall be stored in a secure location at an alternate site accessible by management and other key personnel. Procedures shall be developed, documented, and implemented effectively to respond to contingencies by ensuring separation of routine information system operations and the alternate storage site.

#### 4.6.7. Alternate Processing Site (CP-7)

Agreements with an alternate processing site shall be established and implemented to permit the resumption of CMS information system operations for mission critical business functions when the primary processing capabilities are unavailable, and the CP calls for application recovery in place of other accepted processes. Procedures shall be developed, documented, and implemented effectively to establish contingency activities and responsibilities.

#### 4.6.8. Telecommunications Services (CP-8)

Necessary agreements shall be established and implemented for alternate communications services capable of restoring adequate communications to accomplish mission critical functions when the primary operations and communications capabilities are unavailable.

#### 4.6.9. Information System Backup (CP-9)

Backup mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable the backing-up of user-level and system-level information (including system state information) contained in the CMS information system. The frequency of information system backups and the transfer rate of backup

information to an alternate storage site (if so designated) shall be consistent with the CMS recovery time objectives and recovery point objectives.

Mechanisms shall provide for sufficient backup storage capability. Checkpoint capabilities shall be part of any backup operation that updates files and consumes large amounts of information system time. Backup copies of CMS data shall be created on a regular basis, and appropriate safeguards shall be implemented to protect the technical and physical security of backup media at the storage location. Where appropriate, backup copies of all other forms of data, including paper records, shall be created based upon an assessment of the level of data criticality and the corresponding risk of data loss.

#### 4.6.10. Information System Recovery and Reconstitution (CP-10)

Information system recovery and reconstitution mechanisms with supporting procedures shall be developed, documented, and implemented effectively to allow the CMS information system to be recovered and reconstituted to a known secure state after a disruption or failure. Recovery of CMS information systems after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.

## 4.7 Identification and Authentication (IA)

### 4.7.1. Identification and Authentication Policy and Procedures (IA-1)

Automated IA mechanisms shall be implemented and enforced for all CMS information systems in a manner commensurate with the risk and sensitivity of the system, network, and data. Supporting procedures shall be developed, documented, and implemented effectively to enable reliable identification of individual users of CMS information systems. The IA procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, FIPS 201, NIST SP 800-63, NIST SP 800-73, and NIST SP 800-76.

### 4.7.2. User Identification and Authentication (IA-2)

Automated IA mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable unique IA of individual users (or processes acting in behalf of users) of CMS information systems. Authentication of user identities shall be accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein.

### 4.7.3. Device Identification and Authentication (IA-3)

Automated mechanisms shall be used to enable IA of the CMS information system being used and to which a connection is being made before establishing a connection.

### 4.7.4. Identifier Management (IA-4)

Procedures shall be developed, documented, and implemented effectively to manage user identifiers. The procedures shall address processes and controls for:

- 4.7.4.1. Identifying each user uniquely;
- 4.7.4.2. Verifying the identity of each user;
- 4.7.4.3. Receiving authorization to issue a user identifier from an appropriate organization official;
- 4.7.4.4. Ensuring that the user identifier is issued to the intended party;
- 4.7.4.5. Disabling user identifier after a specific period of inactivity; and
- 4.7.4.6. Archiving user identifiers.

Reviews and validation of system users' accounts shall be conducted to ensure the continued need for access to a system. Identifier management shall not be applicable to shared information system accounts (i.e., guest and anonymous).

#### 4.7.5. Authenticator Management (IA-5)

Procedures shall be developed, documented, and implemented effectively to manage user authenticators. The procedures shall address processes and controls for: initial authenticator content; distribution for new, lost, compromised, or damaged authenticators; revocation of authenticators; changing default authenticators; and changing / refreshing authenticators at specified intervals. Users shall not loan or share authenticators with other users. Lost or compromised authenticators shall be reported immediately to appropriate authority.

Selection of passwords or other authentication devices (e.g., tokens, biometrics) shall be appropriate, based on the CMS System Security Level of the information system. Automated mechanisms shall be in place for password-based authentication, to ensure that the information system:

- 4.7.5.1. Protects passwords from unauthorized disclosure and modification when stored and transmitted;
- 4.7.5.2. Prohibits passwords from being displayed when entered;
- 4.7.5.3. Enforces automatic expiration of passwords;
- 4.7.5.4. Prohibits password reuse for a specified number of generations; and
- 4.7.5.5. Enforces periodic password changes.

#### 4.7.6. Authenticator Feedback (IA-6)

Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to obscure feedback to users during the

authentication process to protect the information from possible exploitation / use by unauthorized individuals.

#### 4.7.7. Cryptographic Module Authentication (IA-7)

Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

## 4.8 Incident Response (IR)

### 4.8.1. Incident Response Policy and Procedures (IR-1)

An IR plan shall be developed, disseminated and reviewed / updated periodically to address the implementation of IR controls. IR procedures shall be developed, documented, and implemented effectively to monitor and respond to all IS incidents or suspected incidents by addressing all critical aspects of incident handling and response containment. The IR procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-61 and current CMS Procedures.

### 4.8.2. Incident Response Training (IR-2)

All personnel shall be trained in their IR roles and responsibilities with respect to a CMS information system. Personnel shall receive periodic refresher training in IR procedures.

### 4.8.3. Incident Response Testing and Exercises (IR-3)

The IR capability for a CMS information system shall be tested periodically using appropriate tests, procedures, automated mechanisms, and exercises to determine the plan's effectiveness. The test results, procedures, and exercises employed to conduct the test shall be documented.

### 4.8.4. Incident Handling (IR-4)

An incident handling capability, which includes preparation, identification, containment, eradication, recovery, and follow-up capabilities in response to security incidents, shall be established and maintained. Evidence of computer crimes, computer misuse, and all other unlawful computer activities shall be properly preserved. Lessons learned from on-going incident handling activities shall be incorporated into the IR procedures.

### 4.8.5. Incident Monitoring (IR-5)

On-going monitoring of the CMS information system for security events shall be conducted. All events and activities associated with system performance shall be monitored for the identification of resources used by processes and user activity that may indicate security threats resulting from user, software, or hardware activity. All information system security

incidents shall be tracked and documented on an on-going basis. All user activities shall be subject to monitoring to verify compliance with this policy and to detect actions that may be in violation of this policy.

#### 4.8.6. Incident Reporting (IR-6)

All IS incidents, or suspected incidents, shall be reported to the CMS IT Service Desk (or equivalent organizational function) as soon as an incident comes to the attention of a user of CMS information or information systems. Events and confirmed security incidents by business partners shall also be reported to the CMS IT Service Desk in accordance with established procedures.

#### 4.8.7. Incident Response Assistance (IR-7)

A CMS IT Service Desk (or equivalent organizational function) shall be in place and shall play an appropriate role in the organization's IR program. The CMS IT Service Desk shall offer advice to users of a CMS information system. Procedures shall be developed, documented, and implemented effectively to facilitate the incident response by providing central incident support resource for CMS information system users.

## 4.9 Maintenance (MA)

#### 4.9.1. System Maintenance Policy and Procedures (MA-1)

System maintenance shall be employed on all CMS information systems addressing critical aspects of hardware and software maintenance including scheduling of controlled periodic maintenance; maintenance tools; remote maintenance; maintenance personnel; and timeliness of maintenance. Maintenance of software shall include the installation of all relevant patches and fixes required to correct security flaws in existing software and to ensure the continuity of business operations.

#### 4.9.2. Controlled Maintenance (MA-2)

Comprehensive maintenance procedures shall be developed, documented, and implemented effectively to conduct controlled periodic on-site and off-site maintenance of the CMS information systems and of the physical plant within which these information systems reside. Controlled maintenance includes, but is not limited to, scheduling, performing, testing, documenting, and reviewing records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Appropriate officials shall approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, all information from associated media shall be removed using CMS-approved procedures. After maintenance is performed on the information system, the security features shall be tested to ensure that they are still functioning properly.

#### 4.9.3. Maintenance Tools (MA-3)

The use of system maintenance tools, including diagnostic and test equipment and administration utilities, shall be approved, controlled, and monitored. Approved tools shall be maintained on an on-going basis.

#### 4.9.4. Remote Maintenance (MA-4)

Remote maintenance of a CMS information system must be approved by the CIO or his/her designated representative. Remote maintenance procedures shall be developed, documented, and implemented effectively to provide additional controls on remotely executed maintenance and diagnostic activities.

The use of remote diagnostic tools shall be described in the SSP for the information system. Maintenance records for all remote maintenance, diagnostic, and service activities shall be maintained and shall be reviewed periodically by appropriate organization officials. All sessions and remote connections shall be terminated after the remote maintenance is completed. If password-based authentication is used during remote maintenance, the passwords shall be changed following each remote maintenance service.

#### 4.9.5. Maintenance Personnel (MA-5)

Maintenance personnel procedures shall be developed, documented, and implemented effectively to control maintenance of CMS information systems. A list of individuals authorized to perform maintenance on the information system shall be maintained.

#### 4.9.6. Timely Maintenance (MA-6)

Maintenance services and parts shall be available in a timely manner.

#### 4.9.7. Off-site Physical Repair of Systems (MA-CMS-1)

Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality.

#### 4.9.8. On-site Physical Repair of Systems (MA-CMS-2)

Controls shall be developed, documented, and implemented effectively to enable on-site physical repair of systems without compromising security functionality or confidentiality.

### **4.10 Media Protection (MP)**

#### 4.10.1. Media Protection Policy and Procedures (MP-1)

MP controls and procedures shall be developed, documented, and implemented effectively to address media access; media labeling; media transport; media destruction; media sanitization and clearing; media storage; and disposition of media records. The MP procedures shall be

consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

#### 4.10.2. Media Access (MP-2)

Procedures shall be developed, documented, and implemented effectively to ensure adequate supervision of personnel and review of their activities to protect against unauthorized receipt, change, or destruction of electronic and paper media based on the sensitivity of the CMS information. Automated mechanisms shall be implemented to control access to media storage areas and to audit access attempts and access granted.

#### 4.10.3. Media Labeling (MP-3)

Storage media and information system output shall have external labels affixed to indicate the distribution limitations, applicable security classification, and handling caveats of the information. Specific types of media or hardware components may be exempted from the labeling requirement, so long as the exempted items remain within a secure environment. Only the CIO or his/her designated representative shall have the authority to exempt specific types of media or hardware components from the labeling requirement.

#### 4.10.4. Media Storage (MP-4)

Media storage procedures shall be developed, documented, and implemented effectively to facilitate the secure storage of media, both electronic and paper, within controlled areas. Storage media shall be controlled physically and safeguarded in the manner prescribed for the highest system security level of the information ever recorded on it until destroyed or sanitized using CMS-approved procedures.

#### 4.10.5. Media Transport (MP-5)

Physical, administrative, and technical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic) to authorized personnel based on the sensitivity of the CMS information.

#### 4.10.6. Media Sanitization and Disposal (MP-6)

Formal documented procedures shall be developed and implemented effectively to ensure that sanitization and disposal methods are commensurate with the sensitivity and criticality of data residing on storage devices, equipment, and hard copy documents. Media sanitization actions shall be tracked, documented, and verified. Sanitization equipment and procedures shall be tested periodically to ensure proper functionality.

Media destruction and disposal procedures shall be developed, documented, and implemented effectively, in an environmentally approved manner, to facilitate the disposal of media, both electronic and paper using approved methods, to ensure that CMS information does not become available to unauthorized personnel. Approved equipment removal procedures for CMS information systems and components that have processed or contained

CMS information shall be followed. Inventory and disposition records for media, both electronic and paper, shall be produced, stored, updated, and retained.

#### 4.10.7. Media Related Records (MP-CMS-1)

Inventory and disposition records for information system media shall be maintained to ensure control and accountability of CMS information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach.

### **4.11 Physical and Environmental Protection (PE)**

#### 4.11.1. Physical and Environmental Protection Policy and Procedures (PE-1)

Physical and environmental protection procedures shall be developed and implemented effectively to protect all CMS IT infrastructure and assets from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft whether accidental or intentional. These procedures shall meet all federal, state and local building codes and be consistent with General Services Administration policies, directives, regulations, and guidelines.

#### 4.11.2. Physical Access Authorizations (PE-2)

Access lists of personnel with authorized access to facilities containing CMS information or information systems (except for those areas within the facilities officially designated as publicly accessible) shall be documented on standard forms, maintained on file, approved by appropriate organizational officials, and reviewed periodically, and, if necessary, updated. Appropriate authorization credentials (e.g., badges, identification cards, smart cards) shall be issued to authorized personnel. Personnel who no longer require access shall be removed promptly from all access lists.

#### 4.11.3. Physical Access Control (PE-3)

Physical access control devices (e.g., keys, locks, combinations, card-readers) and/or guards shall be used to control entry to and exit from facilities containing CMS information or information systems, except for areas and/or facilities officially designated as publicly accessible. Individual access authorizations shall be verified before granting access to facilities containing CMS information or information systems. Physical access control devices (e.g., keys, locks, combinations, key cards) shall be secured and inventoried on a regular basis.

Combinations, access codes, and keys shall be changed promptly when lost, compromised, or when individuals are transferred or terminated. Re-entry to facilities during emergency-related events shall be restricted to authorized individuals only. Access to workstations and associated peripheral computing devices shall be appropriately controlled when located in areas designated as publicly accessible.

#### 4.11.4. Access Control for Transmission Medium (PE-4)

Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering of CMS information system transmission lines within organizational facilities that carry unencrypted information.

#### 4.11.5. Access Control for Display Medium (PE-5)

Physical access controls shall be developed, documented, and implemented effectively to prevent unauthorized individuals from observing CMS sensitive information displayed on information system devices.

#### 4.11.6. Monitoring Physical Access (PE-6)

Physical access to information systems shall be monitored for physical security compliance and to detect and respond to incidents. Appropriate organization officials shall periodically review physical access records, investigate apparent security violations or suspicious physical access activities, and take appropriate remedial action.

#### 4.11.7. Visitor Control (PE-7)

Visitor controls shall be developed, documented, and implemented effectively to control access to sensitive facilities and restricted / controlled areas containing CMS information, information systems, and media libraries. Visitors shall be authenticated prior to being granted access to facilities or areas other than areas designated as publicly accessible. Government contractors and others with permanent authorization credentials are not considered visitors.

#### 4.11.8. Access Records (PE-8)

Visitor access to sensitive facilities and restricted / controlled areas that contain CMS information or information systems shall be logged. The visitor access record shall contain:

4.11.8.1 Name and organization of the person visiting;

4.11.8.2 Signature of the visitor;

4.11.8.3 Form of identification;

4.11.8.4 Date of access;

4.11.8.5 Time of entry and departure;

4.11.8.6 Purpose of visit; and

4.11.8.7 Name and organization of person visited.

Appropriate organization officials shall periodically review the access records, including after closeout.

#### 4.11.9. Power Equipment and Power Cabling (PE-9)

Power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain safe power for CMS information systems.

#### 4.11.10. Emergency Shutoff (PE-10)

Emergency shut-off controls shall be developed, documented, and implemented effectively to provide the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.

#### 4.11.11. Emergency Power (PE-11)

Emergency power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to facilitate an orderly shutdown of the CMS information system in the event of a primary power source loss.

#### 4.11.12. Emergency Lighting (PE-12)

Mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enhance safety and availability. Automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes shall be provided.

#### 4.11.13. Fire Protection (PE-13)

Fire protection mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to prevent, detect, and respond to fire. Fire suppression and detection devices / systems that can be activated in the event of a fire shall be employed and maintained. Fire suppression and detection devices / systems shall include, but not be limited to, sprinkler systems, hand-held fire extinguishers, fixed fire hoses, and smoke detectors.

#### 4.11.14. Temperature and Humidity Controls (PE-14)

Temperature and humidity control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain (within acceptable levels) and monitor the temperature and humidity of facilities containing CMS information systems.

#### 4.11.15. Water Damage Protection (PE-15)

All necessary steps shall be taken to ensure that the building plumbing does not endanger CMS information systems. Procedures shall be developed, documented, and implemented effectively to reduce the potential damage from plumbing leaks.

#### 4.11.16. Delivery and Removal (PE-16)

Procedures shall be developed, documented, and implemented effectively to control the flow of information system-related items into and out of the organization. Appropriate officials shall authorize the delivery or removal of CMS information system-related items.

To avoid unauthorized access, delivery and removal controls shall be implemented to isolate delivery areas from sensitive facilities and restricted / controlled areas containing CMS information, information systems, and media libraries.

#### 4.11.17. Alternate Work Site (PE-17)

Procedures shall be developed, documented, and implemented effectively to control information system security at alternate work sites. A method of communication shall be provided to employees at alternate work sites to report security issues or suspected security incidents.

#### 4.11.18. Location of Information System Components (PE-18)

Procedures shall be developed, documented, and implemented effectively to ensure that information system components are positioned within the facility to minimize potential damage from physical and environmental hazards, and to minimize the opportunity for unauthorized access.

#### 4.11.19. Information Leakage (PE-19)

Safeguards and countermeasures should be considered to protect information systems against information leakage due to electromagnetic signals emanations.

## **4.12 Planning (PL)**

### 4.12.1. Security Planning Policy and Procedures (PL-1)

All CMS information systems and major applications shall be documented in a SSP, which is compliant with OMB Circular A-130 and consistent with NIST SP 800-18. The SSP shall be approved by appropriate organization officials and incorporated into the information resources management strategic plan. The information contained in the SSP is the basis for system accreditation, and subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, in accordance with current CMS Procedures.

#### 4.12.2. System Security Plan (SSP) (PL-2)

All CMS information systems and major applications shall be covered by an SSP, which is compliant with OMB Circular A-130 and consistent with the intent of NIST SP 800-18. The SSP shall document the operation and security requirements of the system / application and the controls in place for meeting those requirements. The SSP shall be approved by appropriate organization officials and incorporated into the information resources management strategic plan. The information contained in the SSP is subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

#### 4.12.3. System Security Plan Update (PL-3)

The SSP shall be reviewed at least every 365 days and updated minimally every three (3) years to reflect current conditions or whenever there are significant changes made to the information system, facilities, or other conditions that may impact security; when the data sensitivity level increases; after a serious security violation; due to changes in the threat environment; or before the previous accreditation expires.

#### 4.12.4. Rules of Behavior (ROB) (PL-4)

ROBs shall be established in alignment HHS requirements <http://hhs.gov/ocio/policy/2008-0001.003s.html>, and made readily available, to delineate clearly user responsibilities and expected behavior of all Business Owners, users, operators, and administrators with regard to information and information system usage. Before authorizing access to the information system and / or information and annually thereafter, the organization shall receive a signed acknowledgement from all users indicating that they have read, understand, and agree to abide by the ROBs. Specific ROBs shall be established to govern work-at-home users who access CMS information or information systems.

Limited personal use of organization-owned or leased equipment and resources shall be considered to be a permitted use of organization-owned or leased equipment and resources when the following conditions are met:

- 4.12.4.1. Such use involves minimal additional expense to CMS;
- 4.12.4.2. Such use does not interfere with the mission or operation of CMS;
- 4.12.4.3. Such use does not violate the Standards of Ethical Conduct for Employees of the Executive Branch;
- 4.12.4.4. Such use does not overburden any CMS information system resources;
- 4.12.4.5. Such use is not otherwise prohibited under this policy; and
- 4.12.4.6. Any use of organizational Internet and email resources shall be made with the understanding that such use is not secure, private or anonymous.

The following uses of organization-owned or leased equipment or resources, either during working or non-working hours, are strictly prohibited:

- 4.12.4.7. Activities that are in violation of law, Government-wide rule or regulation or that are otherwise inappropriate for the workplace;
- 4.12.4.8. Activities that would compromise the security of any Government host computer. This includes, but is not limited to, sharing or disclosing log-on identification and passwords;
- 4.12.4.9. Fund-raising or partisan political activities, endorsements of any products or services or participation in any lobbying activity;
- 4.12.4.10. All email communications to groups of employees that are subject to approval prior to distribution and have not been approved by the organization (e.g., retirement announcements, union notices or announcements, charitable solicitations); and
- 4.12.4.11. Employees shall not use the Internet for any purpose, which would reflect negatively on CMS or its employees.

All employees shall have a reasonable expectation of privacy in the workplace. However, employee users of organization-owned or leased equipment and resources shall not have an expectation of privacy while using such equipment or resources at any time, including times of permitted personal usage as set forth in this policy. To the extent that employees desire to protect their privacy, employees shall not use organization-owned or leased equipment and resources.

#### 4.12.5. Privacy Impact Assessment (PIA) (PL-5)

PIAs shall be conducted for CMS information systems. The PIAs shall be compliant with the E-Government Act of 2002, OMB Memorandum M-03-22, and the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations.

#### 4.12.6. Security-Related Activity Planning (PL-6)

Security-related activities affecting the information system shall be planned and coordinated before being performed in order to reduce the impact on CMS operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing / exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.

## 4.13 Personnel Security (PS)

### 4.13.1. Personnel Security Policy and Procedures (PS-1)

CMS information systems shall employ personnel security controls consistent with applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines. Procedures shall be developed to guide the implementation of personnel security controls.

### 4.13.2. Position Categorization (PS-2)

A criticality / sensitivity rating (e.g., non-sensitive, national security, public trust) shall be assigned to all positions within the organization. The criticality / sensitivity rating shall be in compliance with 5 CFR 731.106(a), Executive Orders 10450 and 12968, NSPD-1, HSPD-7, and HSPD-12 and consistent with OPM policy and guidance. Screening criteria shall be established based on the information system access given to the individuals filling those positions. All positions shall be reviewed periodically for criticality / sensitivity rating. All criticality / sensitivity ratings must be submitted to the DHHS HR department and CMS' personnel security department.

### 4.13.3. Personnel Screening (PS-3)

Prior to being granted access, all employees and contractors who require access to CMS information or information systems shall be screened and reinvestigated periodically, consistent with the criticality / sensitivity rating of the position. For prospective employees, references background checks shall be performed before issuance of a User ID. Security agreements shall be required for employees and contractors assigned to work with mission critical information.

### 4.13.4. Personnel Termination (PS-4)

Termination procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information and information systems is removed upon personnel termination. Termination procedures shall address:

- 4.13.4.1. Exit interviews;
- 4.13.4.2. Retrieval of all organizational information system-related property;
- 4.13.4.3. Notification to security management;
- 4.13.4.4. Revocation of all system access privileges;
- 4.13.4.5. Immediately escorting employees terminated for cause out of organization facilities; and
- 4.13.4.6. Hard disk back up and sanitization before re-issuance.

Appropriate personnel shall have access to official records created by the terminated employee that are stored on organizational information systems.

#### 4.13.5. Personnel Transfer (PS-5)

Transfer procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information or information systems no longer required in the new assignment is terminated upon personnel transfer. Transfer procedures shall address:

4.13.5.1. Re-issuing appropriate organizational information system-related property (e.g., keys, identification cards, building passes);

4.13.5.2. Notification to security management;

4.13.5.3. Closing obsolete accounts and establishing new accounts; and

4.13.5.4. Revocation of all system access privileges (if applicable).

#### 4.13.6. Access Agreements (PS-6)

Individuals who require access to CMS information or information systems shall be required to complete and sign appropriate access agreements, including, but not limited to, non-disclosure agreements, acceptable use agreements, ROBs, and conflict-of-interest agreements.

#### 4.13.7. Third-Party Personnel Security (PS-7)

Personnel security controls employed by external service providers and third parties shall be documented, agreed to, implemented effectively, and monitored for compliance and shall include provisions for security clearances, background checks, required expertise, defined security roles and responsibilities, and confidentiality agreements. Personnel security controls employed by service providers and third parties shall be compliant with CMS IS policies and procedures, and consistent with NIST SP 800-35.

#### 4.13.8. Personnel Sanctions (PS-8)

The organization shall enforce formal personnel sanctions process for personnel who fail to comply with established CMS IS policies and procedures. The employee sanction process shall be consistent with applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines.

#### 4.13.9. Review System Access during Extraordinary Personnel Circumstances (PS-CMS-1)

Access to CMS information and information systems shall be reviewed during extraordinary personnel circumstances and limited as deemed necessary.

#### 4.13.10. Designate an Information System Security Officer (ISSO) / System Security Officer (SSO) (PS-CMS-2)

An Information System Security Officer (ISSO) / System Security Officer (SSO) shall be designated for each business component with roles and responsibilities of the position clearly defined.

### 4.14 Risk Assessment (RA)

#### 4.14.1. Risk Assessment Policy and Procedures (RA-1)

All CMS applications and systems shall be covered by an IS RA. The RA shall be consistent with NIST SP 800-30. Formal documented procedures shall be developed, disseminated, and reviewed / updated periodically to facilitate the implementation of the RA policy and associated RA controls. The procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

#### 4.14.2. Security Categorization (RA-2)

CMS information systems and the information processed, stored, or transmitted by the systems shall be categorized in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to the, *CMS System Security Level by Information Type*. The security categorization (including supporting rationale) shall be explicitly documented. Designated senior-level officials within CMS shall review and approve the security categorizations. CMS shall conduct security categorizations as an organization-wide activity with the involvement of the CMS CIO, CISO, and Business Owners.

All CMS information systems categorized as high or moderate shall be considered sensitive or to contain sensitive information. All CMS information systems categorized as low shall be considered non-sensitive or to contain non-sensitive information. All CMS information systems shall implement minimum security requirements and controls as established in the current CMS IS Standards, based on security categorization of the system.

#### 4.14.3. Risk Assessment (RA-3)

An assessment of risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems that support the operations and assets of CMS shall be performed, both within CMS and by external parties that manage / operate information or information systems for CMS. The RA shall be in accordance with current CMS Procedures. Based on the operation of the information system, the RA shall take into account vulnerabilities, threat sources, and security controls in place to determine the resulting level of residual risk posed to CMS operations, CMS assets, CMS information, or individuals.

Any findings from reviews of CMS systems shall be evaluated as to the impact of the vulnerability on the information system. Any identified weaknesses shall be documented by

the Business Owner or external party and addressed by mitigating the risk, accepting the risk with explanation or submitting Corrective Action Plan (CAP). These findings shall be subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

#### 4.14.4. Risk Assessment Update (RA-4)

The RA shall be performed and documented every three (3) years or whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation.

#### 4.14.5. Vulnerability Scanning (RA-5)

Appropriate vulnerability assessment tools and techniques shall be implemented by the organization. Selected personnel shall be trained in their use and maintenance. The organization shall conduct periodic testing of its security posture by scanning its information systems with vulnerability tools. The information obtained from the vulnerability scanning process shall be shared with appropriate personnel throughout the organization on a “need to know” basis to help eliminate similar vulnerabilities in other information systems. The activities of employees using organization Internet and email resources shall be subject to monitoring by system or security personnel without notice.

### **4.15 System and Services Acquisition (SA)**

#### 4.15.1. System and Services Acquisition Policy and Procedures (SA-1)

Documented procedures shall be developed and implemented effectively to facilitate the implementation of the system and services acquisition security controls in all system and services acquisitions. Procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

#### 4.15.2. Allocation of Resources (SA-2)

As part of the capital planning and investment control processes, CMS or the external organization shall determine, document, and allocate the resources required to protect CMS information systems adequately. IS requirements shall be included in mission / business case planning, and a separate line item shall be established in CMS’ programming and budgeting documentation for the implementation and management of information systems security.

#### 4.15.3. Life Cycle Support (SA-3)

A uniform System Development Life-Cycle (SDLC) methodology shall be established and followed to manage all CMS information systems.

#### 4.15.4. Acquisitions (SA-4)

Security requirements and/or security specifications shall be included, either explicitly or by reference, in all information system acquisition contracts based on an assessment of risk in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

##### Solicitation Documents

Solicitation documents (e.g., Request for Proposal) for any CMS information system shall include, either explicitly or by reference, security requirements that describe the required:

- 4.15.4.1. Security capabilities;
- 4.15.4.2. Design and development processes;
- 4.15.4.3. Test and evaluation procedures; and
- 4.15.4.4. Documentation.

The requirements in the solicitation documents shall permit updating security controls as new threats / vulnerabilities are identified and as new technologies are implemented

##### Use of Evaluated and Validated Products

For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology products, when multiple products meet CMS requirements, preference shall be given to products that have been evaluated and validated through one or more of the following sources:

1. The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme;
2. The International Common Criteria Recognition Arrangements; and
3. The NIST Cryptographic Module Validation Program.

##### Configuration Settings and Implementation Guidance

The information system required documentation shall include security configuration settings, including documentation explaining exceptions to the standard, and security implementation guidance.

#### 4.15.5. Information System Documentation (SA-5)

Procedures shall be developed, documented, and implemented effectively to ensure that adequate documentation for all CMS information systems and its constituent components is available, protected when required, and distributed only to authorized personnel. The administrative and user guides and/or manuals shall include information on configuring, installing, and operating the information system, and for optimizing the system's security features. The guides and/or manuals shall be reviewed periodically, and, if necessary, updated as new vulnerabilities are identified and/or new security controls are added.

#### 4.15.6. Software Usage Restrictions (SA-6)

All software or shareware and associated documentation used on CMS information systems shall be deployed and maintained in accordance with appropriate license agreements and copyright laws. Software associated documentation protected by quantity licenses shall be managed through a tracking system to control copying and distribution. All other uses not specifically authorized by the license agreement shall be prohibited. The use of publicly accessible peer-to-peer file sharing technology shall be controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

#### 4.15.7. User Installed Software (SA-7)

All users shall be restricted from downloading or installing software, unless explicitly authorized in writing by the CIO or his/her designated representative. Users that have been granted such authorization may download and install only organization-approved software. The use of install-on-demand software shall be restricted.

#### 4.15.8. Security Engineering Principles (SA-8)

CMS information systems shall be designed and implemented using accepted security engineering principles.

#### 4.15.9. External Information System Services (SA-9)

All external information system services shall include specific provisions requiring the service provider to comply with CMS IS policies, standards, and guidelines; and shall be monitored for compliance. CMS shall define the remedies for any loss, disruption, or damage caused by the service provider's failure to comply. Service providers shall be prohibited from outsourcing any system function overseas, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representatives with concurrence from CMS' personnel security department.

#### 4.15.10. Developer Configuration Management (SA-10)

Information system developers shall develop, document, and implement a configuration management plan for each information system under development. The configuration management plan shall address change control mechanisms during development, change authorization requirements, and security flaw identification, tracking, and remediation processes.

#### 4.15.11. Developer Security Testing (SA-11)

Information system developers shall develop, document, and implement a security test and evaluation (ST&E) plan for each information system under development in accordance with,

but not limited to the, current CMS Procedures. The developer security test results shall be documented.

## **4.16 System and Communications Protection (SC)**

### **4.16.1. System and Communications Protection Policy and Procedures (SC-1)**

Technical controls shall be developed, documented, and implemented effectively to ensure the CIA of CMS information systems and the protection of the CMS information system communications. Procedures shall be developed, documented, and implemented effectively to guide the implementation and management of such technical controls. The technical controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

### **4.16.2. Application Partitioning (SC-2)**

User interface services (e.g., web services) shall be separated physically or logically from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

### **4.16.3. Security Function Isolation (SC-3)**

Information system security functions shall be isolated from non-security functions by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform those security functions. The system shall maintain a separate execution domain (e.g., address space) for each executing process.

### **4.16.4. Information Remnance (SC-4)**

No information, including encrypted representations of information, produced by a prior user's actions (or the actions of a process acting on behalf of a prior user) shall be available to any current user (or current process) who obtains access to a shared system resource that has been released back to the information system. There shall be no residual information from the shared resource.

### **4.16.5. Denial of Service Protection (SC-5)**

Mechanisms shall be established to prevent, or limit the effects of well-known, detectable, and preventable denial-of-service attacks.

### **4.16.6. Resource Priority (SC-6)**

Mechanisms shall be implemented to provide for allocation of information system resources based upon priority. Priority protection shall ensure that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.

#### 4.16.7. Boundary Protection (SC-7)

Automated boundary protection mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. Any connections to the Internet, or other external networks or information systems, shall occur through controlled interfaces. The operational failure of the boundary protection mechanisms shall not result in any unauthorized release of information outside of the information system boundary. Information system boundary protections at any designated alternate processing site shall provide the same levels of protection as those of the primary site.

#### 4.16.8. Transmission Integrity (SC-8)

Procedures shall be developed and documented, and technical controls shall be established and implemented effectively to protect the integrity of CMS information while in transit.

#### 4.16.9. Transmission Confidentiality (SC-9)

Procedures shall be developed and documented, and technical controls shall be established and implemented effectively to protect the confidentiality of CMS sensitive information while in transit.

#### 4.16.10. Network Disconnect (SC-10)

Technical controls shall be established and implemented effectively to ensure that network connections are properly terminated at the end of user sessions, or upon the occurrence of specified conditions (e.g., a period of inactivity).

#### 4.16.11. Trusted Path (SC-11)

Technical controls shall be established and implemented effectively to provide the capability to establish trusted communications paths between authorized users and the security functionality of the information system.

#### 4.16.12. Cryptographic Key Establishment and Management (SC-12)

When cryptography is required and used within the information system, documented procedures shall be implemented effectively for cryptographic key generation, distribution, storage, use, and destruction. Symmetric and asymmetric keys used to protect sensitive information shall be controlled and distributed using the NIST SP 800-56 and NIST SP 800-57 approved key management guidance.

#### 4.16.13. Use of Cryptography (SC-13)

When cryptographic mechanisms are used, procedures shall be developed, documented, and implemented effectively to ensure they comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. All such mechanisms shall be FIPS 140-2 (as amended and revised) compliant and NIST validated.

#### 4.16.14. Public Access Protections (SC-14)

Technical controls shall be developed, documented, and implemented effectively to protect the integrity of the publicly accessible CMS information and applications.

#### 4.16.15. Collaborative Computing (SC-15)

Running collaborative computing mechanisms on CMS information systems shall require authorization by the CIO or his/her designated representative. The authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which mechanisms can be used. Collaborative computing mechanisms shall not be activated remotely.

#### 4.16.16. Transmission of Security Parameters (SC-16)

Technical controls shall be developed, documented, and implemented effectively to ensure that CMS information systems reliably associate security parameters with information exchanged between information systems.

#### 4.16.17. Public Key Infrastructure Certificates (SC-17)

All public key certificates used within the CMS information system shall be issued in accordance with a defined certification policy and certification practice statement. Registration to receive a public key certificate shall include authorization by a supervisor or a responsible official, and shall be done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

#### 4.16.18. Mobile Code (SC-18)

CMS shall establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause harm to CMS information systems. The organization shall document, monitor, and implement controls for the use of mobile code within the CMS information system. Appropriate officials shall authorize or deny the use of mobile code. The organization shall implement controls and procedures for mobile code in accordance with NIST SP 800-28.

#### 4.16.19. Voice Over Internet Protocol (SC-19)

CMS shall establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to harm CMS information systems. The organization shall document, monitor, and implement controls for the use of VoIP within a

CMS information system. When VoIP is implemented, the organization shall adhere to the NIST SP 800-58 guidance.

4.16.20. Secure Name / Address Resolution Service (Authoritative Source) (SC-20)

Technical controls shall be developed, documented, and implemented effectively to ensure that each information system that provides name / address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

4.16.21. Secure Name / Address Resolution Service (Recursive or Caching Resolver) (SC-21)

Technical controls shall be developed, documented, and implemented effectively to ensure that each information system that provides name / address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.

4.16.22. Architecture and Provisioning for Name / Address Resolution Service (SC-22)

Information systems that collectively provide name / address resolution service for an organization shall be fault tolerant and implement role separation.

4.16.23. Session Authenticity (SC-23)

Technical controls shall be developed, documented, and effectively implemented to ensure that CMS information systems provide mechanisms to protect the authenticity of communications sessions.

4.16.24. Desktop Modems (SC-CMS-1)

Users are prohibited from installing desktop modems.

4.16.25. Identify and Detect Unauthorized Modems (SC-CMS-2)

Automated methods and related procedures shall be established, documented and implemented effectively to identify and detect unauthorized modems.

4.16.26. Secondary Authentication and Encryption (SC-CMS-3)

Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secure network.

4.16.27. Electronic Mail (SC-CMS-4)

Controls shall be developed, documented, and implemented effectively to protect CMS sensitive information that is sent via email.

#### 4.16.28. Persistent Cookies (SC-CMS-5)

The use of persistent cookies on a CMS web site is prohibited unless explicitly approved in writing by the DHHS Secretary.

#### 4.16.29. Network Interconnection (SC-CMS-6)

Controls shall be developed, documented, and implemented effectively to ensure that only properly authorized network interconnections external to the system boundaries are established.

### **4.17 System and Information Integrity (SI)**

#### 4.17.1. System and Information Integrity Policy and Procedures (SI-1)

Automated mechanisms for system, software, and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to systems, software, and information. The procedures and automated mechanisms shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

#### 4.17.2. Flaw Remediation (SI-2)

Information system flaws in an operational CMS information system shall be identified, reported and effective remedial actions shall be taken. Systems affected by recently announced software vulnerabilities shall be identified. Patches, service packs, and hot fixes shall be tested for effectiveness and potential side effects on the CMS information systems prior to installation. The flaw remediation process shall be centrally managed and updates shall be installed automatically without individual user intervention.

#### 4.17.3. Malicious Code Protection (SI-3)

Automated malicious code protection mechanisms that include a capability of automatic updates shall be in place and supporting procedures shall be developed, documented, and implemented effectively to identify and isolate suspected malicious software. Antiviral mechanisms shall be implemented effectively and maintained, at critical information system entry points, and at each workstation, server, or mobile computing device on the network to detect and eradicate malicious code transported by email, email attachments, removable media or other methods. Business Owners shall use antiviral software products from multiple vendors, if possible, and update virus protection mechanisms whenever new releases are available.

#### 4.17.4. Information System Monitoring Tools and Techniques (SI-4)

Effective monitoring tools and techniques providing real-time identification of unauthorized use, misuse, and abuse of the information system shall be implemented.

#### 4.17.5. Security Alerts and Advisories (SI-5)

Procedures shall be developed, documented, and implemented effectively to establish a process for receiving IS alerts and advisories on a regular basis, and for issuing IS alerts and advisories to appropriate personnel. Upon receipt of such alerts and advisories, personnel shall take appropriate response actions. The types of actions to be taken in response to security alerts / advisories shall be documented.

#### 4.17.6. Security Functionality Verification (SI-6)

Automated mechanisms shall be established and implemented effectively to provide the capability for CMS information systems to verify the correct operation of security functions on a regular basis, and automatically to take appropriate response actions when security-related anomalies are discovered.

#### 4.17.7. Software and Information Integrity (SI-7)

Automated mechanisms for software and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to software. Good software engineering practices consistent with CMS IS policy and procedures shall be employed with regard to commercial-off-the-shelf (COTS) integrity mechanisms, and automated mechanisms shall be in place to monitor the integrity of the CMS information system and applications.

#### 4.17.8. Spam Protection (SI-8)

Automated mechanisms for spam protection shall be in place at critical information system entry points, workstations, servers, and mobile computing devices on the network. Supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect spam.

#### 4.17.9. Information Input Restrictions (SI-9)

Automated mechanisms shall be in place to restrict information input to the information system to authorized personnel. Personnel authorized to input information to the information system shall be restricted beyond the typical access controls employed by the system, including limitations based on specific operational / project responsibilities.

#### 4.17.10. Information Accuracy, Completeness, Validity, and Authenticity (SI-10)

Automated mechanisms shall verify information for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.

#### 4.17.11. Error Handling (SI-11)

Information systems shall identify and handle error conditions in an expeditious manner. User error messages generated by information systems shall provide timely and useful information to users without revealing information that could be exploited by adversaries.

System error messages shall be revealed only to authorized personnel. Sensitive information shall not be listed in error logs or associated administrative messages.

#### 4.17.12. Information Output Handling and Retention (SI-12)

Output from information systems shall be handled and retained in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, operational requirements, and the information sensitivity level.

---

## 5. ROLES AND RESPONSIBILITIES

The following entities have responsibilities related to the implementation of this program policy.

### 5.1 CMS Administrator

The CMS Administrator has the overall responsibility for the implementation of an agency-wide IS Program as required by the laws and regulation as directed by the Department of Health and Human Services (DHHS) for ensuring compliance with all government-wide legal and policy requirements.

The CMS Administrator shall be responsible for the following duties, in accordance with provisions of FISMA:

- Providing information security protections commensurate with this policy, the CMS IS program and federal regulations;
- Ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control;
- Delegating to the CMS CIO the authority to ensure compliance with the requirements imposed on CMS under sub-section 3544 of FISMA, Federal Agency Responsibilities;
- Ensuring that CMS has trained personnel sufficient to assist CMS in complying with the requirements of this policy and related procedures, standards and guidelines; and
- Ensuring that the CMS CIO, in coordination with other senior CMS officials, reports annually to the CMS Administrator on the effectiveness of the CMS IS Program, including progress of remedial actions.

### 5.2 CMS Chief Information Officer (CIO)

The CMS CIO is responsible for the following:

- Ensuring there is an appropriate level of protection for all CMS information resources, whether retained in-house or under the control of contractors, including the establishment of operational, management and technical safeguards;
- Assisting Business Owners in understanding their security responsibilities and ensuring that they incorporate an acceptable level of protection for all CMS IT Systems;

- Developing, implementing and administering the CMS IS Program, as well as DHHS and government-wide security directives;
- Designating a Chief Information Security Officer (CISO);
- Developing and maintaining this policy, information security procedures, and control techniques to address federal requirements;
- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and
- Assisting senior agency officials concerning their responsibilities regarding information and information systems that support operations and assets under their realm of responsibility.

### **5.3 Chief Information Security Officer (CISO)**

The CMS CISO is responsible for the following activities:

- Developing and implementing an information system security training and orientation program in accordance with the requirements from the FISMA of 2002;
- Developing, evaluating and providing information about the CMS IS Program, and communicating CMS IS Program requirements and concerns to CMS management and personnel;
- Ensuring that SSPs are developed, reviewed, implemented, and revised;
- Maintaining documentation used to establish systems security level designations for all SSPs within CMS;
- Ensuring that IS RAs are developed, reviewed, and implemented for the SSP process;
- Providing leadership & participating in IS incident response and reporting IS incidents in accordance with reporting procedures developed and implemented by Federal mandates, HHS, and CMS;
- Mediating and resolving systems security issues that arise between two CMS organizations, CMS and other federal organizations, or CMS and States or contractors;
- Assuring that CMS business Component Information System Security Officers (ISSOs) are appointed and trained;
- Assisting CMS business Component ISSOs in developing local systems security; and
- Researching state-of-the-art systems security technology and disseminating information material in a timely fashion.

### **5.4 Component ISSOs**

Component ISSOs are responsible for the following activities:

- Assisting the CISO in ensuring the component adheres to laws, Executive Orders, directives, regulations, policies, standards, and CMS IS Program requirements;

- Serving as the primary point of contact in the component for IS issues; and
- Participating in the technical certification of component RAs and SSPs.

## 5.5 Business Owners

CMS Business Owners are responsible for the following activities:

- Assessing the risk to the information and information systems over which they have responsibility;
- Ensuring, through system certification, that the CMS information systems over which they have responsibility are developed, implemented, operated, and documented according to the requirements of this policy;
- Certifying that CMS information systems fully comply with CMS IS requirements; and
- Ensuring appropriate security measures and supporting documentation are maintained.

## 5.6 System Administrators

System Administrators are responsible for the following activities:

- Verifying that system security requirements of their systems are being met;
- Establishing and communicating the security safeguards required for protecting systems based on the sensitivity levels of the information; and
- Periodically reviewing and verifying that all users of their systems are authorized and are using the required systems security safeguards, in compliance with the CMS IS Program and all related standards, guidelines, and procedures.

## 5.7 System Developers / Maintainers

System Developers/Maintainers are responsible for the following activities:

- Developing and implementing the IS requirements throughout the SDLC; and
- Planning and implementation for the on-going maintenance of the information system, including updates, upgrades and patches in accordance with the SDLC and this policy.

## 5.8 CMS / Business Partner / Contractor Employees

CMS / Business Partner / Contractor employees have the responsibility to ensure the protection of CMS' information (data) and information systems by complying with the IS requirements maintained in this policy and in the *CMS IS "Virtual Handbook"*<sup>1</sup>. Use of organization-owned or leased equipment and resources to accomplish work-related responsibilities will always have priority over personal use. In order to avoid capacity problems and to reduce the susceptibility

---

<sup>1</sup> The *CMS IS "Virtual Handbook"* is the collection of all CMS policies, procedures, standards, and guidelines which implement the CMS IS Program.

of organization information technology resources to computer viruses and cyber attacks, employees shall comply with the following requirements:

- Personal files obtained via the Internet may not be stored on individual PC hard drives or on local area network (LAN) file servers;
- Official video and voice files may not be downloaded from the Internet except when they will be used to serve an approved organization function; and
- Internet and email etiquette, customs and courtesies shall be followed when using organization-owned or leased equipment or resources.

## 5.9 Users

Users have the responsibility to ensure the protection of CMS' information (data) and information systems by complying with the IS requirements maintained in this policy and in the *CMS IS "Virtual Handbook"*. Users shall attend required information security and functional training. In addition, users shall adhere to the duties, requirements and responsibilities as stated in Article 35 of the 2004 MLA or any of its successors.

---

## 6. APPLICABLE LAWS/GUIDANCE

The following public laws and federal guidance are applicable to this policy:

- FISMA Act of 2002, Public Law (P.L.) 107-347;
- HIPAA, 1996, P.L. 104-191;
- Medicare Modernization Act of 2003, P.L. 108-173;
- The Privacy Act of 1974, as amended (5 U.S.C. 552a);
- OMB Circular A-130, Management of Federal Information Resources, November 28, 2000;
- OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, February 28, 2000;
- OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 30, 2003;
- OMB Memorandum M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act, August 23, 2004;
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006;
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007;
- Federal Information Processing Standards (FIPS), Publication 140-2, Security Requirements for Cryptographic Modules, Change Notice 2, December 3, 2002;

- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004;
- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006;
- Federal Preparedness Circulars (FPC) 65, June 15, 2004;
- Federal Preparedness Circulars (FPC) 67, April 30, 2001;
- National Security Presidential Directive (NSPD)-1, February 13, 2001;
- Homeland Security Presidential Directives (HSPD)-7, December 17, 2003;
- Homeland Security Presidential Directives (HSPD)-12, August 27, 2004;
- NIST SP 800-53 Rev. 2, Recommended Security Controls for Federal Information Systems, December 2007, and other NIST 800 Series Special Publications;
- CMS Information Security Policy, CMS-OA-POL-SEC01, April 12, 2006; and
- CMS Policy for Investment Management and Governance, May 17, 2007.

---

## **7. INFORMATION AND ASSISTANCE**

Contact the Director of the Enterprise Architecture and Strategy Group (EASG) within OIS for further information regarding this policy.

---

## **8. EFFECTIVE DATE/IMPLEMENTATION**

This policy becomes effective on the date that CMS' CIO signs it and remains in effect until officially superseded or cancelled by the CMS CIO.

---

## **9. APPROVED**

---

Julie C. Boughn  
CMS Chief Information Officer and  
Director, Office of Information Services

---

Date of Issuance

---

## 10. ASSOCIATED RESOURCES

This policy is augmented by the:

- CMS Information Security "Virtual Handbook," <http://www.cms.hhs.gov/InformationSecurity/>
- CMS Integrated IT Investment and System Lifecycle Framework <http://www.cms.hhs.gov/SystemLifecycleFramework/>
- CMS CIO Directives [http://www.cms.hhs.gov/InfoTechGenInfo/04\\_CIODirectives.asp](http://www.cms.hhs.gov/InfoTechGenInfo/04_CIODirectives.asp)

---

## GLOSSARY

### Automated Labeling

Refers to labels employed on internal data structures (e.g., records, files) within the information system. [NIST SP 800-53R2]

### Automated Marking

Refers to markings employed on external media (e.g., hardcopy documents output from the information system). The markings used in external marking are distinguished from the labels used on internal data structures described in automated labeling [NIST SP 800-53R2]

### Baseline Configuration

Includes information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. Also includes a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs / objectives. [NIST SP 800-53R2]

### Contingency Plan (CP)

Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. The CP provides procedures and capabilities for recovering a major application or general support system. [NIST SP 800-34]

### Cryptographic Key (Key)

A parameter used in conjunction with a cryptographic algorithm that determines:

- the transformation of plaintext data into ciphertext data,

- the transformation of ciphertext data into plaintext data,
- a digital signature computed from data,
- the verification of a digital signature computed from data,
- an authentication code computed from data, or
- an exchange agreement of a shared secret. [FIPS 140-2]

### **Cryptographic Module**

The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. [FIPS 140-2]

### **Incident**

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [NIST SP 800-53R2]

### **Incident Response Plan**

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's IT system(s). [NIST SP 800-34]

### **Information Remnance**

Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user / role (or the actions of a process acting on behalf of a prior user / role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. [NIST SP 800-53R2]

### **Information System Media**

Includes both digital media (e.g., diskettes, magnetic tapes, external / removable hard drives, flash / thumb drives, compact disks [CD], digital video disks [DVD]) and non-digital media (e.g., paper, microfilm). [NIST SP 800-53R2]

### **Key Management**

The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. [FIPS 140-2]

**Malicious Code**

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. [CNSS Inst. 4009 & NIST SP 800-61]

**Media Sanitization**

The process used to remove information from information system media such that there is a reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. [NIST SP 800-53R2]

**Mobile Code**

Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. These software programs include: Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. [NIST SP 800-53R2]

**Portable and Mobile Devices**

This includes notebook computers, personal digital assistants, cellular telephones; and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations. [NIST SP 800-53R2]

**Privacy Impact Assessment (PIA)**

An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. [OMB Memorandum M-03-22]

**Privileged Function**

A function executed on an information system involving the control, monitoring, or administration of the system. [NIST SP 800-53R2]

**Public Key Certificate**

A set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity. [FIPS 140-2]

**Remote Access**

Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. [NIST SP 800-53R2]

### **Remote Maintenance**

Maintenance and diagnostic activities conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). [NIST SP 800-53R2]

### **Remote Session**

A session initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). [NIST SP 800-53R2]

### **Safeguards**

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. [CNSS Inst. 4009]

### **Sanitization**

The process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. [NIST SP 800-53R2]

### **Security Controls**

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [NIST SP 800-53R2]

### **Secure Name / Address Resolution Service (Authoritative Source)**

Enables remote clients to obtain origin authentication and integrity verification assurances for the name / address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name / address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure DNS deployment. [NIST SP 800-53R2]

**Secure Name / Address Resolution Service (Recursive or Caching Resolver)**

An information system that provides name / address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST SP 800-81 provides guidance on secure domain name system deployment. [NIST SP 800-53R2]

**Session**

A session is an encounter between an end-user interface device (e.g., computer, terminal, process) and an application, including a network logon. One user session is the time between starting the application and quitting. [Mixture of sources]

**Sensitive Information**

Information is considered sensitive if the loss of confidentiality, integrity, or availability could be expected to have a serious, severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. [HHS Memorandum ISP-2007-005]

**Significant Change**

Includes, but is not limited to, changes in operating systems, computer hardware, firmware, operational environment, or system boundaries; new services or applications; or other conditions that potentially impact the system's security posture or accreditation status. [NIST SP 800-53R2]

**Spyware**

This is software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. [NIST SP 800-53R2]

**Trusted Path**

A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software. [NIST SP 800-53R2]

**User**

Individual or (system) process authorized to access an information system. [NIST SP 800-53R2]