QECP Data Security Workbook

June 25, 2014

This template is intended to guide organizations through the minimum requirements of the data security standard (Standard 3) under the CMS Qualified Entity Certification Program for Medicare Data (QECP). It includes all CMS requirements that a prospective applicant must meet to become a certified qualified entity (QE) and to maintain their QE status. This workbook is intended to be used as a reference for prospective QE applicants and a compliance tool for certified QEs when submitting their data security evidence.

QEs must provide evidence of rigorous data privacy and security policies, including enforcement mechanisms, for any information systems that will contain CMS data.

The information requested within this workbook is required by CMS in order to comply with the Federal Information Security Management Act (FISMA), NIST 800-53, and must be completed in detail in order for the QECP team to assess QEs' security environment maturity level. Currently, all Medicare fee-for-service (FFS) data that will be released to certified QEs under the CMS QE program requires a security classification of "Moderate." Appendix B of the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) details all the security controls for systems with a rating of "Moderate." The direct link to the Appendix B of the ARS is below:
http://www.cms.gov/informationsecurity/downloads/ARS_App_B_CMSR_Moderate.pdf

This workbook has been condensed into individual tabs specific to each control family (e.g., access control, incident response) and grouped by QECP Element (3A, 3B, and 3C).

For each control, QEs must either complete the **green Compliance Description** cells (for Primary Controls) or self-attest in the **gray Compliance Description** cells and the **Compliance pull-down menu** (for Secondary Controls) (see examples below). Responses should explain how the QE is meeting the requirements for each control. In addition to this workbook, relevant detailed documentation in support of each control should be uploaded to the QE's application portal and mapped to the control for which it is supporting. Please note that, **at a minimum**, you are required to submit separate detailed documentation for 18 of the primary security controls that ask you to describe your organization's general policies and procedures for each security family. Specifically, you are required to upload independent documentation that demonstrates your compliance with the following 18 security controls:

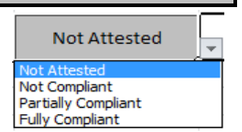
AU-1, CA-1, IR-1, PL-1, RA-1, AC-1, AT-1, CM-1, IA-1, PS-1, CP-1, MA-1, MP-1, PE-1, SA-1, SC-1, SI-1 and PM-1.

Beyond these 18 controls, we strongly recommend (but are not requiring) that you provide additional documentation for all other primary controls. Once completed, your responses in this workbook and your additional documentation will be reviewed by the QECP data security team for appropriateness.

Upon submission, this workbook is considered sensitive information and must be treated as such. Do not email this information. Only use secure, approved methods to transport this workbook.

Compliance Description:
Enter compliance response in these cells.

Compliance Description:
Enter self-attestation comments in these cells then use the drop down box to to the right to attest to your level of Compliance.



(QE's Company Name Here) - QECP Controls Review Dashboard

Element 3A

Audit and Accountability

AU-1	NEEDS RESPONSE	NOT REVIEWED
AU-2 wEn	SELF ATTEST	NOT ATTESTED
AU-3 wEn	SELF ATTEST	NOT ATTESTED
AU-4	SELF ATTEST	NOT ATTESTED
AU-5	SELF ATTEST	NOT ATTESTED
AU-6 wEn	SELF ATTEST	NOT ATTESTED
AU-7 wEn	SELF ATTEST	NOT ATTESTED
AU-8 wEn	SELF ATTEST	NOT ATTESTED
AU-9 wEn	SELF ATTEST	NOT ATTESTED
AU-10	SELF ATTEST	NOT ATTESTED
AU-11	SELF ATTEST	NOT ATTESTED
AU-12 wEn	SELF ATTEST	NOT ATTESTED

Security Assessment and Authorization

CA-1	NEEDS RESPONSE	NOT REVIEWED
CA-2 wEn	SELF ATTEST	NOT ATTESTED
CA-3 wEn	NEEDS RESPONSE	NOT REVIEWED
CA-5 wEn	SELF ATTEST	NOT ATTESTED
CA-6	SELF ATTEST	NOT ATTESTED
CA-7 wEn	SELF ATTEST	NOT ATTESTED
CA-9	SELF ATTEST	NOT ATTESTED

Incident Response

IR-1	NEEDS RESPONSE	NOT REVIEWED
IR-2	SELF ATTEST	NOT ATTESTED
IR-3 wEn	SELF ATTEST	NOT ATTESTED
IR-4 wEn	SELF ATTEST	NOT ATTESTED
IR-5	SELF ATTEST	NOT ATTESTED
IR-6 wEn	SELF ATTEST	NOT ATTESTED
IR-7 wEn	SELF ATTEST	NOT ATTESTED
IR-8	SELF ATTEST	NOT ATTESTED

Planning

PL-1	NEEDS RESPONSE	NOT REVIEWED
PL-2 wEn	SELF ATTEST	NOT ATTESTED
PL-4 wEn	NEEDS RESPONSE	NOT REVIEWED
PL-8	SELF ATTEST	NOT ATTESTED

Risk Assessment

RA-1	NEEDS RESPONSE	NOT REVIEWED
RA-2	SELF ATTEST	NOT ATTESTED
RA-3	SELF ATTEST	NOT ATTESTED
RA-5 wEn	SELF ATTEST	NOT ATTESTED

NOTE: wEn = Control has additional Enhanced Controls and **All Enhancement Controls must be Compliant or Satisfied to report as Compliant/Satisfied on Dashboard.

Element 3B

Access Control

AC-1	NEEDS RESPONSE	NOT REVIEWED
AC-2 wEn	NEEDS RESPONSE	NOT REVIEWED
AC-3 wEn	NEEDS RESPONSE	NOT REVIEWED
AC-4	SELF ATTEST	Not Attested
AC-5	SELF ATTEST	Not Attested
AC-6 wEn	NEEDS RESPONSE	NOT REVIEWED
AC-7	SELF ATTEST	NOT ATTESTED
AC-8	SELF ATTEST	NOT ATTESTED
AC-10	SELF ATTEST	NOT ATTESTED
AC-11 wEn	NEEDS RESPONSE	NOT REVIEWED
AC-12	SELF ATTEST	NOT ATTESTED
AC-14	SELF ATTEST	NOT ATTESTED
AC-16	SELF ATTEST	NOT ATTESTED
AC-17 wEn	SELF ATTEST	NOT ATTESTED
AC-18 wEn	SELF ATTEST	NOT ATTESTED
AC-19 wEn	SELF ATTEST	NOT ATTESTED
AC-20 wEn	SELF ATTEST	NOT ATTESTED
AC-21	SELF ATTEST	NOT ATTESTED
AC-22	SELF ATTEST	NOT ATTESTED

Security Awareness and Training

AT-1	NEEDS RESPONSE	NOT REVIEWED
AT-2 wEn	SELF ATTEST	NOT ATTESTED
AT-3	NEEDS RESPONSE	NOT REVIEWED
AT-4	NEEDS RESPONSE	NOT REVIEWED

Configuration Management

CM-1	NEEDS RESPONSE	NOT REVIEWED
CM-2 wEn	SELF ATTEST	NOT ATTESTED
CM-3 wEn	SELF ATTEST	NOT ATTESTED
CM-4 wEn	SELF ATTEST	NOT ATTESTED
CM-5 wEn	SELF ATTEST	NOT ATTESTED
CM-6 wEn	SELF ATTEST	NOT ATTESTED
CM-7 wEn	SELF ATTEST	NOT ATTESTED
CM-8 wEn	SELF ATTEST	NOT ATTESTED
CM-9	SELF ATTEST	NOT ATTESTED
CM-10	SELF ATTEST	NOT ATTESTED
CM-11	SELF ATTEST	NOT ATTESTED

Identification and Authentication

IA-1	NEEDS RESPONSE	NOT REVIEWED
IA-2 wEn	SELF ATTEST	NOT ATTESTED
IA-3	SELF ATTEST	NOT ATTESTED
IA-4 wEn	SELF ATTEST	NOT ATTESTED
IA-5 wEn	SELF ATTEST	NOT ATTESTED
IA-6	SELF ATTEST	NOT ATTESTED
IA-7	SELF ATTEST	NOT ATTESTED
IA-8 wEn	NEEDS RESPONSE	NOT REVIEWED

Personnel Security

PS-1	NEEDS RESPONSE	NOT REVIEWED
PS-2	NEEDS RESPONSE	NOT REVIEWED
PS-3	SELF ATTEST	NOT ATTESTED
PS-4	NEEDS RESPONSE	NOT REVIEWED
PS-5	SELF ATTEST	NOT ATTESTED
PS-6	NEEDS RESPONSE	NOT REVIEWED
PS-7	SELF ATTEST	NOT ATTESTED
PS-8	SELF ATTEST	NOT ATTESTED

NOTE: wEn = Control has additional Enhanced Controls and **All Enhancement Controls must be Compliant or Satisfied to report as Compliant/Satisfied on Dashboard.

Element 3C

Contingency Planning

CP-1	NEEDS RESPONSE	NOT REVIEWED
CP-2 wEn	SELF ATTEST	NOT ATTESTED
CP-3	SELF ATTEST	Not Attested
CP-4 wEn	SELF ATTEST	NOT ATTESTED
CP-6 wEn	SELF ATTEST	NOT ATTESTED
CP-7 wEn	SELF ATTEST	NOT ATTESTED
CP-8 wEn	SELF ATTEST	NOT ATTESTED
CP-9 wEn	SELF ATTEST	NOT ATTESTED
CP-10 wEn	SELF ATTEST	NOT ATTESTED

Maintenance

MA-1	NEEDS RESPONSE	NOT REVIEWED
MA-2	SELF ATTEST	NOT ATTESTED
MA-3 wEn	SELF ATTEST	NOT ATTESTED
MA-4 wEn	SELF ATTEST	NOT ATTESTED
MA-5	SELF ATTEST	NOT ATTESTED
MA-6	SELF ATTEST	NOT ATTESTED

Media Protection

MP-1	NEEDS RESPONSE	NOT REVIEWED
MP-2	NEEDS RESPONSE	NOT REVIEWED
MP-3	NEEDS RESPONSE	NOT REVIEWED
MP-4	NEEDS RESPONSE	NOT REVIEWED
MP-5 wEn	NEEDS RESPONSE	NOT REVIEWED
MP-6 wEn	NEEDS RESPONSE	NOT REVIEWED
MP-7 wEn	NEEDS RESPONSE	NOT REVIEWED
MP-CMS-1	NEEDS RESPONSE	NOT REVIEWED

Physical and Environmental Protection

PE-1	NEEDS RESPONSE	NOT REVIEWED
PE-2	SELF ATTEST	NOT ATTESTED
PE-3	SELF ATTEST	NOT ATTESTED
PE-4	SELF ATTEST	NOT ATTESTED
PE-5	SELF ATTEST	NOT ATTESTED
PE-6 wEn	SELF ATTEST	NOT ATTESTED
PE-8	SELF ATTEST	NOT ATTESTED
PE-9	SELF ATTEST	NOT ATTESTED
PE-10	SELF ATTEST	NOT ATTESTED
PE-11	SELF ATTEST	NOT ATTESTED
PE-12	SELF ATTEST	Not Attested
PE-13 wEn	SELF ATTEST	NOT ATTESTED
PE-14	SELF ATTEST	NOT ATTESTED
PE-15	SELF ATTEST	Not Attested
PE-16	NEEDS RESPONSE	NOT REVIEWED
PE-17	SELF ATTEST	NOT ATTESTED
PE-18	SELF ATTEST	NOT ATTESTED

System and Communications Protection

SC-1	NEEDS RESPONSE	NOT REVIEWED
SC-2	NEEDS RESPONSE	NOT REVIEWED
SC-4	NEEDS RESPONSE	NOT REVIEWED
SC-5	SELF ATTEST	NOT ATTESTED
SC-6	SELF ATTEST	NOT ATTESTED
SC-7 wEn	NEEDS RESPONSE	NOT REVIEWED
SC-8 wEn	NEEDS RESPONSE	NOT REVIEWED
SC-10	NEEDS RESPONSE	NOT REVIEWED
SC-11	SELF ATTEST	NOT ATTESTED
SC-12 wEn	SELF ATTEST	NOT ATTESTED
SC-13	SELF ATTEST	NOT ATTESTED
SC-15 wEn	SELF ATTEST	NOT ATTESTED
SC-17	SELF ATTEST	NOT ATTESTED
SC-18	SELF ATTEST	NOT ATTESTED
SC-19	SELF ATTEST	NOT ATTESTED
SC-20	SELF ATTEST	NOT ATTESTED
SC-21	SELF ATTEST	NOT ATTESTED
SC-22	SELF ATTEST	NOT ATTESTED
SC-23	NEEDS RESPONSE	NOT REVIEWED
SC-28	NEEDS RESPONSE	NOT REVIEWED
SC-30	SELF ATTEST	NOT ATTESTED
SC-32	SELF ATTEST	NOT ATTESTED
SC-39	SELF ATTEST	NOT ATTESTED
SC-CMS-1	SELF ATTEST	NOT ATTESTED
SC-CMS-2	SELF ATTEST	NOT ATTESTED

System and Services Acquisition

SA-1	NEEDS RESPONSE	NOT REVIEWED
SA-2	SELF ATTEST	NOT ATTESTED
SA-3	NEEDS RESPONSE	NOT REVIEWED
SA-4 wEn	SELF ATTEST	NOT ATTESTED
SA-5	SELF ATTEST	NOT ATTESTED
SA-8	SELF ATTEST	NOT ATTESTED
SA-9 wEn	NEEDS RESPONSE	NOT REVIEWED
SA-10	SELF ATTEST	NOT ATTESTED
SA-11 wEn	SELF ATTEST	NOT ATTESTED
SA-12	SELF ATTEST	NOT ATTESTED

System and Information Integrity

SI-1	NEEDS RESPONSE	NOT REVIEWED
SI-2 wEn	SELF ATTEST	NOT ATTESTED
SI-3 wEn	SELF ATTEST	NOT ATTESTED
SI-4 wEn	NEEDS RESPONSE	NOT REVIEWED
SI-5	NEEDS RESPONSE	NOT REVIEWED
SI-6	SELF ATTEST	NOT ATTESTED
SI-7 wEn	SELF ATTEST	NOT ATTESTED
SI-8 wEn	SELF ATTEST	NOT ATTESTED
SI-10	SELF ATTEST	NOT ATTESTED
SI-11	SELF ATTEST	NOT ATTESTED
SI-12	SELF ATTEST	NOT ATTESTED

NOTE: wEn = Control has additional Enhanced Controls and **All Enhancement Controls must be Compliant or Satisfied to report as Compliant/Satisfied on Dashboard.

Element 3C - Management and Privacy

Program Management

PM-1	NEEDS RESPONSE	NOT REVIEWED
PM-2	NEEDS RESPONSE	NOT REVIEWED
PM-3	SELF ATTEST	NOT ATTESTED
PM-4	SELF ATTEST	NOT ATTESTED
PM-5	SELF ATTEST	NOT ATTESTED
PM-6	SELF ATTEST	NOT ATTESTED
PM-7	SELF ATTEST	NOT ATTESTED
PM-8	SELF ATTEST	NOT ATTESTED
PM-9	SELF ATTEST	NOT ATTESTED
PM-10	SELF ATTEST	NOT ATTESTED
PM-11	SELF ATTEST	NOT ATTESTED
PM-12	SELF ATTEST	NOT ATTESTED
PM-13	SELF ATTEST	NOT ATTESTED
PM-14	SELF ATTEST	NOT ATTESTED
PM-15	SELF ATTEST	NOT ATTESTED
PM-16	SELF ATTEST	NOT ATTESTED

Authority and Purpose

AP-1	SELF ATTEST	NOT ATTESTED
AP-2	SELF ATTEST	NOT ATTESTED

Accountability, Audit, and Risk Management

AR-1	SELF ATTEST	NOT ATTESTED
AR-2	SELF ATTEST	NOT ATTESTED
AR-3	SELF ATTEST	NOT ATTESTED
AR-4	SELF ATTEST	NOT ATTESTED
AR-5	SELF ATTEST	NOT ATTESTED
AR-6	SELF ATTEST	NOT ATTESTED
AR-7	SELF ATTEST	NOT ATTESTED
AR-8	SELF ATTEST	NOT ATTESTED

Data Quality and Integrity

DI-1 wEn	SELF ATTEST	NOT ATTESTED
DI-2 wEn	SELF ATTEST	NOT ATTESTED

Data Minimization and Retention

DM-1 wEn	SELF ATTEST	NOT ATTESTED
DM-2 wEn	SELF ATTEST	NOT ATTESTED
DM-3 wEn	SELF ATTEST	NOT ATTESTED

Individual Participation and Redress

IP-1 wEn	SELF ATTEST	NOT ATTESTED
IP-2	SELF ATTEST	NOT ATTESTED
IP-3	SELF ATTEST	NOT ATTESTED
IP-4 wEn	SELF ATTEST	NOT ATTESTED

Security

SE-1	SELF ATTEST	NOT ATTESTED
SE-2	SELF ATTEST	NOT ATTESTED

Transparency

TR-1 wEn	SELF ATTEST	NOT ATTESTED
TR-2 wEn	SELF ATTEST	NOT ATTESTED
TR-3	SELF ATTEST	NOT ATTESTED

Use Limitation

UL-1	SELF ATTEST	NOT ATTESTED
UL-2	SELF ATTEST	NOT ATTESTED

Control #	Control Name	Family	Element	Control Classification
AC-1	**Access Control Policy and Procedures**	**Access Control**	**3B**	**Primary**
AC-2	**Account Management**	**Access Control**	**3B**	**Primary**
AC-2 (1)	account management | automated system account management	Access Control	3B	Primary – Enhancement
AC-2 (2)	account management | removal of temporary / emergency accounts	Access Control	3B	Primary – Enhancement
AC-2 (3)	account management | disable inactive accounts	Access Control	3B	Primary – Enhancement
AC-2 (4)	account management | automated audit actions	Access Control	3B	Primary – Enhancement
AC-2 (7)	account management | role-based schemes	Access Control	3B	Primary – Enhancement
AC-3	**Access Enforcement**	**Access Control**	**3B**	**Primary**
AC-3 (3)	access enforcement | mandatory access control	Access Control	3B	Primary – Enhancement
AC-4	Information Flow Enforcement	Access Control	3B	Secondary
AC-5	Separation of Duties	Access Control	3B	Secondary
AC-6	**Least Privilege**	**Access Control**	**3B**	**Primary**
AC-6 (1)	least privilege | authorize access to security functions	Access Control	3B	Primary – Enhancement
AC-6 (2)	least privilege | non-privileged access for nonsecurity functions	Access Control	3B	Primary – Enhancement
AC-6 (5)	least privilege | privileged accounts	Access Control	3B	Primary – Enhancement
AC-6 (9)	least privilege | auditing use of privileged functions	Access Control	3B	Primary – Enhancement
AC-6 (10)	least privilege | prohibit non-privileged users from executing privileged functions	Access Control	3B	Primary – Enhancement
AC-7	Unsuccessful Logon Attempts	Access Control	3B	Secondary
AC-8	System Use Notification	Access Control	3B	Secondary
AC-10	Concurrent Session Control	Access Control	3B	Secondary
AC-11	**Session Lock**	**Access Control**	**3B**	**Primary**
AC-11 (1)	session lock | pattern-hiding displays	Access Control	3B	Primary – Enhancement
AC-12	Session Termination	Access Control	3B	Secondary
AC-14	Permitted Actions without Identification or Authentication	Access Control	3B	Secondary
AC-16	Security Attributes	Access Control	3B	Secondary
AC-17	Remote Access	Access Control	3B	Secondary
AC-17 (1)	remote access | automated monitoring / control	Access Control	3B	Secondary – Enhancement
AC-17 (2)	remote access | protection of confidentiality / integrity using encryption	Access Control	3B	Secondary – Enhancement
AC-17 (3)	remote access | managed access control points	Access Control	3B	Secondary – Enhancement
AC-17 (4)	remote access | privileged commands / access	Access Control	3B	Secondary – Enhancement
AC-18	Wireless Access	Access Control	3B	Secondary
AC-18 (1)	wireless access | authentication and encryption	Access Control	3B	Secondary – Enhancement
AC-19	Access Control for Mobile Devices	Access Control	3B	Secondary
AC-20	Use of External Information Systems	Access Control	3B	Secondary
AC-20 (1)	use of external information systems | limits on authorized use	Access Control	3B	Secondary – Enhancement
AC-20 (2)	use of external information systems | portable storage devices	Access Control	3B	Secondary – Enhancement
AC-21	Information Sharing	Access Control	3B	Secondary
AC-22	Publicly Accessible Content	Access Control	3B	Secondary
AP-1	Authority to Collect	Authority and Purpose	3C	Secondary
AP-2	Purpose Specification	Authority and Purpose	3C	Secondary
AR-1	Governance and Privacy Program	Accountability, Audit, and Risk Management	3C	Secondary
AR-2	Privacy Impact and Risk Assessment	Accountability, Audit, and Risk Management	3C	Secondary
AR-3	Privacy Requirements for Contractors and Service Providers	Accountability, Audit, and Risk Management	3C	Secondary
AR-4	Privacy Monitoring and Auditing	Accountability, Audit, and Risk Management	3C	Secondary
AR-5	Privacy Awareness and Training	Accountability, Audit, and Risk Management	3C	Secondary
AR-6	Privacy Reporting	Accountability, Audit, and Risk Management	3C	Secondary
AR-7	Privacy-Enhanced System Design and Development	Accountability, Audit, and Risk Management	3C	Secondary
AR-8	Accounting of Disclosures	Accountability, Audit, and Risk Management	3C	Secondary
AT-1	**Security Awareness and Training Policy and Procedures**	**Security Awareness and Training**	**3B**	**Primary**
AT-2	Security Awareness Training	Security Awareness and Training	3B	Secondary
AT-2 (2)	security awareness | insider threat	Security Awareness and Training	3B	Secondary – Enhancement
AT-3	**Role-Based Security Training**	**Security Awareness and Training**	**3B**	**Primary**
AT-4	**Security Training Records**	**Security Awareness and Training**	**3B**	**Primary**
AU-1	**Audit and Accountability Policy and Procedures**	**Audit and Accountability**	**3A**	**Primary**
AU-2	Audit Events	Audit and Accountability	3A	Secondary
AU-2 (3)	audit events | reviews and updates	Audit and Accountability	3A	Secondary – Enhancement
AU-3	Content of Audit Records	Audit and Accountability	3A	Secondary
AU-3 (1)	content of audit records | additional audit information	Audit and Accountability	3A	Secondary – Enhancement
AU-4	Audit Storage Capacity	Audit and Accountability	3A	Secondary
AU-5	Response to Audit Processing Failures	Audit and Accountability	3A	Secondary
AU-6	Audit Review, Analysis, and Reporting	Audit and Accountability	3A	Secondary
AU-6 (1)	audit review, analysis, and reporting | process integration	Audit and Accountability	3A	Secondary – Enhancement
AU-6 (3)	audit review, analysis, and reporting | correlate audit repositories	Audit and Accountability	3A	Secondary – Enhancement
AU-7	Audit Reduction and Report Generation	Audit and Accountability	3A	Secondary
AU-7 (1)	audit reduction and report generation | automatic processing	Audit and Accountability	3A	Secondary – Enhancement
AU-8	Time Stamps	Audit and Accountability	3A	Secondary
AU-8 (1)	time stamps | synchronization with authoritative time source	Audit and Accountability	3A	Secondary – Enhancement
AU-9	Protection of Audit Information	Audit and Accountability	3A	Secondary
AU-9 (2)	protection of audit information | audit backup on separate physical systems / components	Audit and Accountability	3A	Secondary – Enhancement
AU-9 (4)	protection of audit information | access by subset of privileged users	Audit and Accountability	3A	Secondary – Enhancement
AU-10	Non-repudiation	Audit and Accountability	3A	Secondary
AU-11	Audit Record Retention	Audit and Accountability	3A	Secondary
AU-12	Audit Generation	Audit and Accountability	3A	Secondary
AU-12 (1)	audit generation | system-wide / time-correlated audit trail	Audit and Accountability	3A	Secondary – Enhancement
CA-1	**Security Assessment and Authorization Policies and Procedures**	**Security Assessment and Authorization**	**3A**	**Primary**
CA-2	Security Assessments	Security Assessment and Authorization	3A	Secondary
CA-2 (1)	security assessments | independent assessors	Security Assessment and Authorization	3A	Secondary – Enhancement
CA-3	**System Interconnections**	**Security Assessment and Authorization**	**3A**	**Primary**
CA-3 (5)	system interconnections | restrictions on external system connections	Security Assessment and Authorization	3A	Primary – Enhancement
CA-5	Plan of Action and Milestones	Security Assessment and Authorization	3A	Secondary
CA-5 (1)	plan of action and milestones | automation support for accuracy / currency	Security Assessment and Authorization	3A	Secondary – Enhancement
CA-6	Security Authorization	Security Assessment and Authorization	3A	Secondary
CA-7	Continuous Monitoring	Security Assessment and Authorization	3A	Secondary
CA-7 (1)	continuous monitoring | independent assessment	Security Assessment and Authorization	3A	Secondary – Enhancement
CA-9	Internal System Connections	Security Assessment and Authorization	3A	Secondary
CM-1	**Configuration Management Policy and Procedures**	**Configuration Management**	**3B**	**Primary**
CM-2	Baseline Configuration	Configuration Management	3B	Secondary
CM-2 (1)	baseline configuration | reviews and updates	Configuration Management	3B	Secondary – Enhancement
CM-2 (3)	baseline configuration | retention of previous configurations	Configuration Management	3B	Secondary – Enhancement
CM-2 (7)	baseline configuration | configure systems, components, or devices for high-risk areas	Configuration Management	3B	Secondary – Enhancement
CM-3	Configuration Change Control	Configuration Management	3B	Secondary
CM-3 (2)	configuration change control | test / validate / document changes	Configuration Management	3B	Secondary – Enhancement
CM-4	Security Impact Analysis	Configuration Management	3B	Secondary
CM-4 (1)	security impact analysis | separate test environments	Configuration Management	3B	Secondary – Enhancement
CM-4 (2)	security impact analysis | verification of security functions	Configuration Management	3B	Secondary – Enhancement
CM-5	Access Restrictions for Change	Configuration Management	3B	Secondary
CM-5 (1)	access restrictions for change | automated access enforcement / auditing	Configuration Management	3B	Secondary – Enhancement
CM-5 (5)	access restrictions for change | limit production / operational privileges	Configuration Management	3B	Secondary – Enhancement
CM-6	Configuration Settings	Configuration Management	3B	Secondary
CM-6 (1)	configuration settings | automated central management / application / verification	Configuration Management	3B	Secondary – Enhancement
CM-7	Least Functionality	Configuration Management	3B	Secondary

CM-7 (1)	least functionality | periodic review	Configuration Management	3B	Secondary – Enhancement
CM-7 (2)	least functionality | prevent program execution	Configuration Management	3B	Secondary – Enhancement
CM-7 (4)	least functionality | unauthorized software / blacklisting	Configuration Management	3B	Secondary – Enhancement
CM-8	Information System Component Inventory	Configuration Management	3B	Secondary
CM-8 (1)	information system component inventory | updates during installations / removals	Configuration Management	3B	Secondary – Enhancement
CM-8 (3)	information system component inventory | automated unauthorized component detection	Configuration Management	3B	Secondary – Enhancement
CM-8 (5)	information system component inventory | no duplicate accounting of components	Configuration Management	3B	Secondary – Enhancement
CM-9	Configuration Management Plan	Configuration Management	3B	Secondary
CM-10	Software Usage Restrictions	Configuration Management	3B	Secondary
CM-11	User-Installed Software	Configuration Management	3B	Secondary
CP-1	**Contingency Planning Policy and Procedures**	**Contingency Planning**	**3C**	**Primary**
CP-2	Contingency Plan	Contingency Planning	3C	Secondary
CP-2 (1)	contingency plan | coordinate with related plans	Contingency Planning	3C	Secondary – Enhancement
CP-2 (2)	contingency plan | capacity planning	Contingency Planning	3C	Secondary – Enhancement
CP-2 (3)	contingency plan | resume essential missions / business functions	Contingency Planning	3C	Secondary – Enhancement
CP-2 (8)	contingency plan | identify critical assets	Contingency Planning	3C	Secondary – Enhancement
CP-3	Contingency Training	Contingency Planning	3C	Secondary
CP-4	Contingency Plan Testing	Contingency Planning	3C	Secondary
CP-4 (1)	contingency plan testing | coordinate with related plans	Contingency Planning	3C	Secondary – Enhancement
CP-6	Alternate Storage Site	Contingency Planning	3C	Secondary
CP-6 (1)	alternate storage site | separation from primary site	Contingency Planning	3C	Secondary – Enhancement
CP-6 (3)	alternate storage site | accessibility	Contingency Planning	3C	Secondary – Enhancement
CP-7	Alternate Processing Site	Contingency Planning	3C	Secondary
CP-7 (1)	alternate processing site | separation from primary site	Contingency Planning	3C	Secondary – Enhancement
CP-7 (2)	alternate processing site | accessibility	Contingency Planning	3C	Secondary – Enhancement
CP-7 (3)	alternate processing site | priority of service	Contingency Planning	3C	Secondary – Enhancement
CP-8	Telecommunications Services	Contingency Planning	3C	Secondary
CP-8 (1)	telecommunications services | priority of service provisions	Contingency Planning	3C	Secondary – Enhancement
CP-8 (2)	telecommunications services | single points of failure	Contingency Planning	3C	Secondary – Enhancement
CP-9	Information System Backup	Contingency Planning	3C	Secondary
CP-9 (1)	information system backup | testing for reliability / integrity	Contingency Planning	3C	Secondary – Enhancement
CP-9 (3)	information system backup | separate storage for critical information	Contingency Planning	3C	Secondary – Enhancement
CP-10	Information System Recovery and Reconstitution	Contingency Planning	3C	Secondary
CP-10 (2)	information system recovery and reconstitution | transaction recovery	Contingency Planning	3C	Secondary – Enhancement
DI-1	Data Quality	Data Quality and Integrity	3C	Secondary
DI-1(1)	Validate PII - Enhancement	Data Quality and Integrity	3C	Secondary – Enhancement
DI-1(2)	Re-Validate PII - Enhancement	Data Quality and Integrity	3C	Secondary – Enhancement
DI-2	Data Integrity and Data Integrity Board	Data Quality and Integrity	3C	Secondary
DI-2 (1)	Publish Agreements on Website - Enhancement	Data Quality and Integrity	3C	Secondary – Enhancement
DM-1	Minimization of Personally Identifiable Information	Data Minimization and Retention	3C	Secondary
DM-1(1)	Locate/Remove/Redact/Anonymize PII - Enhancement	Data Minimization and Retention	3C	Secondary – Enhancement
DM-2	Data Retention and Disposal	Data Minimization and Retention	3C	Secondary
DM-2(1)	System Configuration - Enhancement	Data Minimization and Retention	3C	Secondary – Enhancement
DM-3	Minimization of PII Used in Testing, Training, and Research	Data Minimization and Retention	3C	Secondary
DM-3(1)	Risk Minimization Techniques - Enhancement	Data Minimization and Retention	3C	Secondary – Enhancement
IA-1	**Identification and Authentication Policy and Procedures**	**Identification and Authentication**	**3B**	**Primary**
IA-2	Identification and Authentication (Organizational Users)	Identification and Authentication	3B	Secondary
IA-2 (1)	identification and authentication (organizational users) | network access to privileged acco	Identification and Authentication	3B	Secondary – Enhancement
IA-2 (2)	identification and authentication (organizational users) | network access to non-privileged	Identification and Authentication	3B	Secondary – Enhancement
IA-2 (3)	identification and authentication (organizational users) | local access to privileged accounts	Identification and Authentication	3B	Secondary – Enhancement
IA-2 (8)	identification and authentication (organizational users) | network access to privileged acco	Identification and Authentication	3B	Secondary – Enhancement
IA-2 (11)	identification and authentication (organizational users) | remote access - separate device	Identification and Authentication	3B	Secondary – Enhancement
IA-2 (12)	identification and authentication (organizational users) | acceptance of piv credentials	Identification and Authentication	3B	Secondary – Enhancement
IA-3	Device Identification and Authentication	Identification and Authentication	3B	Secondary
IA-4	Identifier Management	Identification and Authentication	3B	Secondary
IA-4 (4)	identifier management | identify user status	Identification and Authentication	3B	Secondary – Enhancement
IA-5	Authenticator Management	Identification and Authentication	3B	Secondary
IA-5 (1)	authenticator management | password-based authentication	Identification and Authentication	3B	Secondary – Enhancement
IA-5 (2)	authenticator management | pki-based authentication	Identification and Authentication	3B	Secondary – Enhancement
IA-5 (3)	authenticator management | in-person or trusted third-party registration	Identification and Authentication	3B	Secondary – Enhancement
IA-5 (6)	authenticator management | protection of authenticators	Identification and Authentication	3B	Secondary – Enhancement
IA-5 (7)	authenticator management | no embedded unencrypted static authenticators	Identification and Authentication	3B	Secondary – Enhancement
IA-5 (11)	authenticator management | hardware token-based authentication	Identification and Authentication	3B	Secondary – Enhancement
IA-6	Authenticator Feedback	Identification and Authentication	3B	Secondary
IA-7	Cryptographic Module Authentication	Identification and Authentication	3B	Secondary
IA-8	**Identification and Authentication (Non-Organizational Users)**	**Identification and Authentication**	**3B**	**Primary**
IA-8 (1)	identification and authentication (non-organizational users) | acceptance of piv credentials	Identification and Authentication	3B	Primary – Enhancement
IA-8 (2)	identification and authentication (non-organizational users) | acceptance of third-party cre	Identification and Authentication	3B	Primary – Enhancement
IA-8 (3)	identification and authentication (non-organizational users) | use of ficam-approved produ	Identification and Authentication	3B	Primary – Enhancement
IA-8 (4)	identification and authentication (non-organizational users) | use of ficam-issued profiles	Identification and Authentication	3B	Primary – Enhancement
IP-1	Consent	Individual Participation and Redress	3C	Secondary
IP-1(1)	Mechanisms Supporting Itemized or Tiered Consent - Enhancement	Individual Participation and Redress	3C	Secondary – Enhancement
IP-2	Individual Access	Individual Participation and Redress	3C	Secondary
IP-3	Redress	Individual Participation and Redress	3C	Secondary
IP-4	Complaint Management	Individual Participation and Redress	3C	Secondary
IP-4(1)	Reponse Times - Enhancement	Individual Participation and Redress	3C	Secondary – Enhancement
IR-1	**Incident Response Policy and Procedures**	**Incident Response**	**3A**	**Primary**
IR-2	Incident Response Training	Incident Response	3A	Secondary
IR-3	Incident Response Testing	Incident Response	3A	Secondary
IR-3 (2)	incident response testing | coordination with related plans	Incident Response	3A	Secondary – Enhancement
IR-4	Incident Handling	Incident Response	3A	Secondary
IR-4 (1)	incident handling | automated incident handling processes	Incident Response	3A	Secondary – Enhancement
IR-5	Incident Monitoring	Incident Response	3A	Secondary
IR-6	Incident Reporting	Incident Response	3A	Secondary
IR-6 (1)	incident reporting | automated reporting	Incident Response	3A	Secondary – Enhancement
IR-7	Incident Response Assistance	Incident Response	3A	Secondary
IR-7 (1)	incident response assistance | automation support for availability of information / support	Incident Response	3A	Secondary – Enhancement
IR-7 (2)	incident response assistance | coordination with external providers	Incident Response	3A	Secondary – Enhancement
IR-8	Incident Response Plan	Incident Response	3A	Secondary
MA-1	**System Maintenance Policy and Procedures**	**Maintenance**	**3C**	**Primary**
MA-2	Controlled Maintenance	Maintenance	3C	Secondary
MA-3	Maintenance Tools	Maintenance	3C	Secondary
MA-3 (1)	maintenance tools | inspect tools	Maintenance	3C	Secondary – Enhancement
MA-3 (2)	maintenance tools | inspect media	Maintenance	3C	Secondary – Enhancement
MA-3 (3)	maintenance tools | prevent unauthorized removal	Maintenance	3C	Secondary – Enhancement
MA-4	Nonlocal Maintenance	Maintenance	3C	Secondary
MA-4 (1)	nonlocal maintenance | auditing and review	Maintenance	3C	Secondary – Enhancement
MA-4 (2)	nonlocal maintenance | document nonlocal maintenance	Maintenance	3C	Secondary – Enhancement
MA-4 (3)	nonlocal maintenance | comparable security / sanitization	Maintenance	3C	Secondary – Enhancement
MA-5	Maintenance Personnel	Maintenance	3C	Secondary
MA-6	Timely Maintenance	Maintenance	3C	Secondary
MP-1	**Media Protection Policy and Procedures**	**Media Protection**	**3C**	**Primary**
MP-2	**Media Access**	**Media Protection**	**3C**	**Primary**
MP-3	**Media Marking**	**Media Protection**	**3C**	**Primary**
MP-4	**Media Storage**	**Media Protection**	**3C**	**Primary**
MP-5	**Media Transport**	**Media Protection**	**3C**	**Primary**
MP-5 (4)	media transport | cryptographic protection	Media Protection	3C	Primary – Enhancement

MP-6	**Media Sanitization**	**Media Protection**	**3C**	**Primary**
MP-6 (1)	media sanitization | review / approve / track / document / verify	Media Protection	3C	Primary – Enhancement
MP-6 (2)	media sanitization | equipment testing	Media Protection	3C	Primary – Enhancement
MP-7	**Media Use**	**Media Protection**	**3C**	**Primary**
MP-7 (1)	media use | prohibit use without owner	Media Protection	3C	Primary – Enhancement
MP-CMS-1	**Media Related Records**	**Media Protection**	**3C**	**Primary**
PE-1	**Physical and Environmental Protection Policy and Procedures**	**Physical and Environmental Protection**	**3C**	**Primary**
PE-2	Physical Access Authorizations	Physical and Environmental Protection	3C	Secondary
PE-3	Physical Access Control	Physical and Environmental Protection	3C	Secondary
PE-4	Access Control for Transmission Medium	Physical and Environmental Protection	3C	Secondary
PE-5	Access Control for Output Devices	Physical and Environmental Protection	3C	Secondary
PE-6	Monitoring Physical Access	Physical and Environmental Protection	3C	Secondary
PE-6 (1)	monitoring physical access | intrusion alarms / surveillance equipment	Physical and Environmental Protection	3C	Secondary – Enhancement
PE-8	Visitor Access Records	Physical and Environmental Protection	3C	Secondary
PE-9	Power Equipment and Cabling	Physical and Environmental Protection	3C	Secondary
PE-10	Emergency Shutoff	Physical and Environmental Protection	3C	Secondary
PE-11	Emergency Power	Physical and Environmental Protection	3C	Secondary
PE-12	Emergency Lighting	Physical and Environmental Protection	3C	Secondary
PE-13	Fire Protection	Physical and Environmental Protection	3C	Secondary
PE-13 (1)	fire protection | detection devices / systems	Physical and Environmental Protection	3C	Secondary – Enhancement
PE-13 (2)	fire protection | suppression devices / systems	Physical and Environmental Protection	3C	Secondary – Enhancement
PE-13 (3)	fire protection | automatic fire suppression	Physical and Environmental Protection	3C	Secondary – Enhancement
PE-14	Temperature and Humidity Controls	Physical and Environmental Protection	3C	Secondary
PE-15	Water Damage Protection	Physical and Environmental Protection	3C	Secondary
PE-16	**Delivery and Removal**	**Physical and Environmental Protection**	**3C**	**Primary**
PE-17	Alternate Work Site	Physical and Environmental Protection	3C	Secondary
PE-18	Location of Information System Components	Physical and Environmental Protection	3C	Secondary
PL-1	**Security Planning Policy and Procedures**	**Planning**	**3A**	**Primary**
PL-2	System Security Plan	Planning	3A	Secondary
PL-2 (3)	system security plan | plan / coordinate with other organizational entities	Planning	3A	Secondary – Enhancement
PL-4	**Rules of Behavior**	**Planning**	**3A**	**Primary**
PL-4 (1)	rules of behavior | social media and networking restrictions	Planning	3A	Primary – Enhancement
PL-8	Information Security Architecture	Planning	3A	Secondary
PM-1	**Information Security Program Plan**	**Program Management**	**3C**	**Primary**
PM-2	**Senior Information Security Officer**	**Program Management**	**3C**	**Primary**
PM-3	Information Security Resources	Program Management	3C	Secondary
PM-4	Plan of Action and Milestones Process	Program Management	3C	Secondary
PM-5	Information System Inventory	Program Management	3C	Secondary
PM-6	Information Security Measures of Performance	Program Management	3C	Secondary
PM-7	Enterprise Architecture	Program Management	3C	Secondary
PM-8	Critical Infrastructure Plan	Program Management	3C	Secondary
PM-9	Risk Management Strategy	Program Management	3C	Secondary
PM-10	Security Authorization Process	Program Management	3C	Secondary
PM-11	Mission/Business Process Definition	Program Management	3C	Secondary
PM-12	Insider Threat Program	Program Management	3C	Secondary
PM-13	Information Security Workforce	Program Management	3C	Secondary
PM-14	Testing, Training, and Monitoring	Program Management	3C	Secondary
PM-15	Contacts with Security Groups and Associations	Program Management	3C	Secondary
PM-16	Threat Awareness Program	Program Management	3C	Secondary
PS-1	**Personnel Security Policy and Procedures**	**Personnel Security**	**3B**	**Primary**
PS-2	**Position Risk Designation**	**Personnel Security**	**3B**	**Primary**
PS-3	Personnel Screening	Personnel Security	3B	Secondary
PS-4	**Personnel Termination**	**Personnel Security**	**3B**	**Primary**
PS-5	Personnel Transfer	Personnel Security	3B	Secondary
PS-6	**Access Agreements**	**Personnel Security**	**3B**	**Primary**
PS-7	Third-Party Personnel Security	Personnel Security	3B	Secondary
PS-8	Personnel Sanctions	Personnel Security	3B	Secondary
RA-1	**Risk Assessment Policy and Procedures**	**Risk Assessment**	**3A**	**Primary**
RA-2	Security Categorization	Risk Assessment	3A	Secondary
RA-3	Risk Assessment	Risk Assessment	3A	Secondary
RA-5	Vulnerability Scanning	Risk Assessment	3A	Secondary
RA-5 (1)	vulnerability scanning | update tool capability	Risk Assessment	3A	Secondary – Enhancement
RA-5 (2)	vulnerability scanning | update by frequency / prior to new scan / when identified	Risk Assessment	3A	Secondary – Enhancement
RA-5 (3)	vulnerability scanning | breadth / depth of coverage	Risk Assessment	3A	Secondary – Enhancement
RA-5 (5)	vulnerability scanning | privileged access	Risk Assessment	3A	Secondary – Enhancement
RA-5 (6)	vulnerability scanning | automated trend analyses	Risk Assessment	3A	Secondary – Enhancement
SA-1	**System and Services Acquisition Policy and Procedures**	**System and Services Acquisition**	**3C**	**Primary**
SA-2	Allocation of Resources	System and Services Acquisition	3C	Secondary
SA-3	**System Development Life Cycle**	**System and Services Acquisition**	**3C**	**Primary**
SA-4	Acquisition Process	System and Services Acquisition	3C	Secondary
SA-4 (1)	acquisition process | functional properties of security controls	System and Services Acquisition	3C	Secondary – Enhancement
SA-4 (2)	acquisition process | design / implementation information for security controls	System and Services Acquisition	3C	Secondary – Enhancement
SA-4 (7)	acquisition process | NIAP -Approved Protection Profiles	System and Services Acquisition	3C	Secondary – Enhancement
SA-4 (9)	acquisition process | functions / ports / protocols / services in use	System and Services Acquisition	3C	Secondary – Enhancement
SA-4 (10)	acquisition process | use of approved piv products	System and Services Acquisition	3C	Secondary – Enhancement
SA-5	Information System Documentation	System and Services Acquisition	3C	Secondary
SA-8	Security Engineering Principles	System and Services Acquisition	3C	Secondary
SA-9	**External Information System Services**	**System and Services Acquisition**	**3C**	**Primary**
SA-9 (1)	external information systems | risk assessments / organizational approvals	System and Services Acquisition	3C	Primary – Enhancement
SA-9 (2)	external information systems | identification of functions / ports / protocols / services	System and Services Acquisition	3C	Primary – Enhancement
SA-10	Developer Configuration Management	System and Services Acquisition	3C	Secondary
SA-11	Developer Security Testing and Evaluation	System and Services Acquisition	3C	Secondary
SA-11 (1)	developer security testing and evaluation | static code analysis	System and Services Acquisition	3C	Secondary – Enhancement
SA-12	Supply Chain Protection	System and Services Acquisition	3C	Secondary
SC-1	**System and Communications Protection Policy and Procedures**	**System and Communications Protection**	**3C**	**Primary**
SC-2	**Application Partitioning**	**System and Communications Protection**	**3C**	**Primary**
SC-4	**Information in Shared Resources**	**System and Communications Protection**	**3C**	**Primary**
SC-5	Denial of Service Protection	System and Communications Protection	3C	Secondary
SC-6	Resource Availability	System and Communications Protection	3C	Secondary
SC-7	**Boundary Protection**	**System and Communications Protection**	**3C**	**Primary**
SC-7 (3)	boundary protection | access points	System and Communications Protection	3C	Primary – Enhancement
SC-7 (4)	boundary protection | external telecommunications services	System and Communications Protection	3C	Primary – Enhancement
SC-7 (5)	boundary protection | deny by default / allow by exception	System and Communications Protection	3C	Primary – Enhancement
SC-7 (7)	boundary protection | prevent split tunneling for remote devices	System and Communications Protection	3C	Primary – Enhancement
SC-7 (8)	boundary protection | route traffic to authenticated proxy servers	System and Communications Protection	3C	Primary – Enhancement
SC-7 (12)	boundary protection | host-based protection	System and Communications Protection	3C	Primary – Enhancement
SC-7 (13)	boundary protection | isolation of security tools / mechanisms / support components	System and Communications Protection	3C	Primary – Enhancement
SC-7 (18)	boundary protection | fail secure	System and Communications Protection	3C	Primary – Enhancement
SC-8	**Transmission Confidentiality and Integrity**	**System and Communications Protection**	**3C**	**Primary**
SC-8 (1)	transmission confidentiality and integrity | cryptographic or alternate physical protection	System and Communications Protection	3C	Primary – Enhancement
SC-8 (2)	transmission confidentiality and integrity | pre / post transmission handling	System and Communications Protection	3C	Primary – Enhancement
SC-10	**Network Disconnect**	**System and Communications Protection**	**3C**	**Primary**
SC-11	Trusted Path	System and Communications Protection	3C	Secondary
SC-12	Cryptographic Key Establishment and Management	System and Communications Protection	3C	Secondary
SC-12 (2)	cryptographic key establishment and management | symmetric keys	System and Communications Protection	3C	Secondary – Enhancement
SC-13	Cryptographic Protection	System and Communications Protection	3C	Secondary
SC-15	Collaborative Computing Devices	System and Communications Protection	3C	Secondary

SC-15 (1)	collaborative computing devices | physical disconnect	System and Communications Protection	3C	Secondary – Enhancement
SC-17	Public Key Infrastructure Certificates	System and Communications Protection	3C	Secondary
SC-18	Mobile Code	System and Communications Protection	3C	Secondary
SC-19	Voice Over Internet Protocol	System and Communications Protection	3C	Secondary
SC-20	Secure Name /Address Resolution Service	System and Communications Protection	3C	Secondary
SC-21	Secure Name /Address Resolution Service	System and Communications Protection	3C	Secondary
SC-22	Architecture and Provisioning for	System and Communications Protection	3C	Secondary
SC-23	**Session Authenticity**	**System and Communications Protection**	**3C**	**Primary**
SC-28	**Protection of Information at Rest**	**System and Communications Protection**	**3C**	**Primary**
SC-30	Concealment and Misdirection	System and Communications Protection	3C	Secondary
SC-32	Information System Partitioning	System and Communications Protection	3C	Secondary
SC-39	Process Isolation	System and Communications Protection	3C	Secondary
SC-CMS-1	Electronic Mail	System and Communications Protection	3C	Secondary
SC-CMS-2	Website Usage	System and Communications Protection	3C	Secondary
SE-1	Inventory of Personally Identifiable Information	Security	3C	Secondary
SE-2	Privacy Incident Response	Security	3C	Secondary
SI-1	**System and Information Integrity Policy and Procedures**	**System and Information Integrity**	**3C**	**Primary**
SI-2	Flaw Remediation	System and Information Integrity	3C	Secondary
SI-2 (1)	flaw remediation | central management	System and Information Integrity	3C	Secondary – Enhancement
SI-2 (2)	flaw remediation | automated flaw remediation status	System and Information Integrity	3C	Secondary – Enhancement
SI-3	Malicious Code Protection	System and Information Integrity	3C	Secondary
SI-3 (1)	malicious code protection | central management	System and Information Integrity	3C	Secondary – Enhancement
SI-3 (2)	malicious code protection | automatic updates	System and Information Integrity	3C	Secondary – Enhancement
SI-4	**Information System Monitoring**	**System and Information Integrity**	**3C**	**Primary**
SI-4 (1)	information system monitoring | system-wide intrusion detection system	System and Information Integrity	3C	Primary – Enhancement
SI-4 (2)	information system monitoring | automated tools for real-time analysis	System and Information Integrity	3C	Primary – Enhancement
SI-4 (4)	information system monitoring | inbound and outbound communications traffic	System and Information Integrity	3C	Primary – Enhancement
SI-4 (5)	information system monitoring | system-generated alerts	System and Information Integrity	3C	Primary – Enhancement
SI-5	**Security Alerts, Advisories, and Directives**	**System and Information Integrity**	**3C**	**Primary**
SI-6	Security Function Verification	System and Information Integrity	3C	Secondary
SI-7	Software, Firmware, and Information Integrity	System and Information Integrity	3C	Secondary
SI-7 (1)	software, firmware, and information integrity | integrity checks	System and Information Integrity	3C	Secondary – Enhancement
SI-7 (7)	software, firmware, and information integrity | integration of detection and response	System and Information Integrity	3C	Secondary – Enhancement
SI-8	Spam Protection	System and Information Integrity	3C	Secondary
SI-8 (1)	spam protection | central management	System and Information Integrity	3C	Secondary – Enhancement
SI-8 (2)	spam protection | automatic updates	System and Information Integrity	3C	Secondary – Enhancement
SI-10	Information Input Validation	System and Information Integrity	3C	Secondary
SI-11	Error Handling	System and Information Integrity	3C	Secondary
SI-12	Information Handling and Retention	System and Information Integrity	3C	Secondary
TR-1	Privacy Notice	Transparency	3C	Secondary
TR-1(1)	Real-Time or Layered Notice - Enhancement	Transparency	3C	Secondary – Enhancement
TR-2	System of Records Notices and Privacy Act Statements	Transparency	3C	Secondary
TR-2(1)	Public Website Publication - Enhancement	Transparency	3C	Secondary – Enhancement
TR-3	Dissemination of Privacy Program Information	Transparency	3C	Secondary
UL-1	Internal Use	Use Limitation	3C	Secondary
UL-2	Information Sharing with Third Parties	Use Limitation	3C	Secondary

Audit and

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Audit and Accountability (AU) Controls

AU-1 - Audit and Accountability Policy and Procedures

CMS ARS Mod 2.0 Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
b. Reviews and updates (as necessary) the current:
1. Audit and accountability policy within every three hundred sixty-five (365) days; and
2. Audit and accountability procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

AU-1 Compliance Description:

AU-2 - Auditable Events

CMS ARS Mod 2.0 Control:
The organization:
a. Determines, based on a risk assessment and CMS mission/business needs, that the information system is capable of auditing the events specified in Implementation Standard 1;
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d. Determines which events specified in Implementation Standard 2 require auditing on a continuous basis in response to specific situations.

Implementation Standard(s)
1. List of auditable events:
(a) Server alerts and error messages;
(b) User log-on and log-off (successful or unsuccessful);
(c) All system administration activities;
(d) Modification of privileges and access;
(e) Start up and shut down;
(f) Application modifications;
(g) Application alerts and error messages;
(h) Configuration changes;
(i) Account creation, modification, or deletion;
(j) File creation and deletion;
(k) Read access to sensitive information;
(l) Modification to sensitive information; and
(m) Printing sensitive information.
2. Subset of Implementation Standard 1 auditable events:
(a) User log-on and log-off (successful or unsuccessful);
(b) All system administration activities;
(c) Modification of privileges and access; and
(d) Account creation, modification, or deletion.

4. (For FTI only) Generate audit records for the following events in addition to those specified in other controls:
(a) All successful and unsuccessful authorization attempts.
(b) All changes to logical access control authorities (e.g., rights, permissions).
(c) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
(d) The audit trail shall capture the enabling or disabling of audit report generation services.
(e) The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).
5. (For CSP only) For service providers, this Standard replaces the above Control and Standards. The organization:
a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events; and for Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes; and
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: organization-defined subset of the auditable events to be audited continually.
6. **(For CSP only)** For service providers, the organization defines the subset of auditable events from AU-2a to be audited. The events to be audited are approved and accepted by Joint Authorization Board (JAB).

Guidance
An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures.

AU-2 Compliance Description:

AU-2(3) - Reviews and Updates – Enhancement

CMS ARS Mod 2.0 Control:
The organization reviews and updates the list of auditable events within every three hundred sixty-five (365) days.

Implementation Standard(s)
1. (For CSP only) For service providers, this Standard replaces the above Enhancement. The organization reviews and updates the list of auditable events annually or whenever there is a change in the threat environment.

Guidance
Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.
(For CSP only) Annually or whenever service provider changes in the threat environment are communicated to the service provider by the Joint Authorization Board (JAB).

AU-2(3) Compliance Description:

AU-3 - Content of Audit Records

CMS ARS Mod 2.0 Control:
The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Implementation Standard(s)
1. **(For PHI only)** Record disclosures of sensitive information, including protected health and financial information. Log information type, date, time, receiving party, and releasing party. Verify within every ninety (90) days for each extract that the data is erased or its use is still required.

Guidance
Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred).

AU-3 Compliance Description:

AU-3(1) - Additional Audit Information – Enhancement

CMS ARS Mod 2.0 Control:
The information system generates audit records containing the following additional, more detailed information:
- Filename accessed;
- Program or command used to initiate the event; and
- Source and destination addresses.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The information system includes additional, more detailed session, connection, transaction, or activity duration information; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon in the audit records for audit events identified by type, location, or subject.
2. **(For CSP only)** For service providers, the organization defines audit record types. The audit record types are approved and accepted by the Joint Authorization Board (JAB).

Guidance
Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. **(For CSP only)** For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.

AU-3(1) Compliance Description:

AU-4 - Audit Storage Capacity

CMS ARS Mod 2.0 Control:
The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Guidance
The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

AU-4 Compliance Description:

AU-5 – Response to Audit Processing Failures

CMS ARS Mod 2.0 Control:
The information system:
a. Alerts defined personnel or roles (defined in the applicable security plan) in the event of an audit processing failure; and
b. Takes the following additional actions in response to an audit failure or audit storage capacity issue:
- Shutdown the information system,
- Stop generating audit records, or
- Overwrite the oldest records, in the case that storage media is unavailable.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the information system takes the following actions in the event of an audit processing failure: shut down.

Guidance
Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

AU-5 Compliance Description:

AU-6 – Audit Review, Analysis, and Reporting

CMS ARS Mod 2.0 - Control:
The organization:
a. Reviews and analyzes information system audit records regularly for indications of inappropriate or unusual activity; and
b. Reports findings to defined personnel or roles (defined in the applicable security plan).

Implementation Standard(s)
1. Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical personnel review and assessment.
2. Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical personnel review and assessment.
3. Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.
4. Use automated utilities to review audit records at least once weekly for unusual, unexpected, or suspicious behavior.
5. Inspect administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created.
6. Perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days.
7. **(For FTI only)** All requests for return information, including receipt and/or disposal of returns or return information, shall be maintained in a log. (see IRS Pub. 1075, sect 6.3.1)
8. **(For CSP only)** For service providers, the organization reviews and analyzes information system audit records at least weekly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials.

Guidance
Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority.

AU-6 Compliance Description:

AU-6(1) - Process Integration – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Guidance
Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits.

AU-6(1) Compliance Description:

AU-6(3) - Correlate Audit Repositories – Enhancement

CMS ARS Mod 2.0 - Control:
The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Guidance
Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness.

AU-6(3) Compliance Description:

AU-7 Audit Reduction and Report Generation

CMS ARS Mod 2.0 - Control:
The information system provides an audit reduction and report generation capability that:
a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
b. Does not alter the original content or time marking of audit records.

Guidance
Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient.

AU-7 Compliance Description:

AU-7(1) - Automatic Processing – Enhancement

CMS ARS Mod 2.0 - Control:
The information system provides the capability to process audit records for events of interest based on selectable event criteria.

Guidance
Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component.

AU-7(1) Compliance Description:

AU-8 Time Stamps

CMS ARS Mod 2.0 - Control:
The information system:
a. Uses internal system clocks to generate time stamps for audit records; and
b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and is accurate to within thirty (30) seconds.

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

AU-8 Compliance Description:

AU-8(1) - Synchronization with Authoritative Time Source – Enhancement

CMS ARS Mod 2.0 - Control:
The information system:
(a) Compares the internal information system clocks daily and at system boot with one or more of the following Federally maintained NTP stratum-1 servers:
- NIST Internet Time Servers (http://tf.nist.gov/tf-cgi/servers.cgi)
- U.S. Naval Observatory Stratum-1 NTP Servers (http://tycho.usno.navy.mil/ntp.html); and
(b) Synchronizes the internal clocks to the authoritative time source when the time difference is greater than thirty (30) seconds.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the information system synchronizes internal information system clocks at least hourly with: http://tf.nist.gov/tf-cgi/servers.cgi.
2. **(For CSP only)** For service providers, the organization selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.
3. **(For CSP only)** For service providers, the organization synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.

Guidance
This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.
(For CSP Only) Synchronization of system clocks improves the accuracy of log analysis.

AU-8(1) Compliance Description:

AU-9 – Protection of Audit Information

CMS ARS Mod 2.0 - Control:
The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Guidance
Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls.

AU-9 Compliance Description:

AU-9(2) - Audit Backup on Separate Physical Systems/Components – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the information system backs up audit records at least weekly onto a physically different system or system component than the system component being audited.

Guidance
(For CSP only) This control enhancement helps to ensure that a compromise of the information system being audited does not also result in a compromise of the audit records.

AU-9(2) Compliance Description:

AU-9(4) - Access by Subset of Privileged Users – Enhancement

CMS ARS Mod 2.0 - Control:
The organization authorizes access to management of audit functionality to only those individuals or roles who are not subject to audit by that system, and is defined in the applicable security plan.

Guidance
Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

AU-9(4) Compliance Description:

AU-10 – Non-Repudiation

CMS ARS Mod 2.0 - Control:
The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed a particular action.

Guidance
Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

AU-10 Compliance Description:

AU-11 – Audit Record Retention

CMS ARS Mod 2.0 - Control:
The organization retains audit records for ninety (90) days and archive old records for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and CMS information retention requirements.

Implementation Standard(s)
1. **(For FTI only)** Employ a permanent system of standardized records of request for disclosure of FTI and maintain the records for five (5) years or the applicable records control schedule, whichever is longer.
2. **(For FTI only)** To support the audit of FTI activities, all organizations must ensure that audit information is archived for six (6) years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored.
3. **(For PII only)** Audit inspection reports, including a record of corrective actions, shall be retained by the organization for a minimum of three (3) years from the date the inspection was completed.
4. **(For CSP only)** For service providers, the organization retains audit records on-line for at least ninety (90) days and further preserves audit records off-line for a period that is in accordance with NARA requirements.

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

AU-11 Compliance Description:

AU-12 – Audit Generation

CMS ARS Mod 2.0 - Control:
The information system:
a. Provides audit record generation capability for the following auditable events defined in AU-2a:
- All successful and unsuccessful authorization attempts.
- All changes to logical access control authorities (e.g., rights, permissions).
- All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
- The audit trail shall capture the enabling or disabling of audit report generation services.
- The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).
b. Allows defined personnel or roles (defined in the applicable security plan) to select which auditable events are to be audited by specific components of the information system;
and
c. Generates audit records for the list of events defined in AU-2d with the content defined in AU-3.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the information system provides audit record generation capability for the list of auditable events defined in AU-2 at all information system components where audit capability is deployed.

Guidance
Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records.

AU-12 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Security Assessment and Authorization Controls (CA)

CA-1 – Security Assessment and Authorization Policies and Procedures

CMS ARS Mod 2.0 - Control
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
b. Reviews and updates (as necesssary) the current:
1. Security assessment and authorization policy within every three hundred sixty-five (365) days; and
2. Security assessment and authorization procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

CA-1 Compliance Description:

CA-2 – Security Assessments

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops a security assessment plan that describes the scope of the assessment including:
1. Security controls and control enhancements under assessment;
2. Assessment procedures to be used to determine security control effectiveness; and
3. Assessment environment, assessment team, and assessment roles and responsibilities;
b. Assesses the security controls in the information system and its environment of operation within every three hundred sixty-five (365) days in accordance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements (CMSR) Standard, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
c. Produces a security assessment report that documents the results of the assessment; and
d. Provides the results of the security control assessment within every three hundred sixty-five (365) days, in writing, to the Business Owner who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system.

Implementation Standard(s)
1. An independent security assessment of all security controls must be conducted prior to issuing the authority to operate for all newly implemented, or significantly changed, systems.
2. The annual security assessment requirement mandated by OMB requires all CMSRs attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period.
3. The Business Owner notifies the CMS CISO within thirty (30) days whenever updates are made to system security authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, ISSO).

Guidance
Organizations assess security controls in organizational information system and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from NIST 800-53 Appendix F (main catalog) and NIST 800-53 Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by CMS, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.
To satisfy annual assessment requirements, organizations can use assessment results from the following sources, including but not limited to: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness; and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the security control selection criteria and subsequently selects a subset of the security controls within the information system and its environment of operation for assessment. Those security controls that are the most volatile (i.e., controls most affected by ongoing changes to the information system or its environment of operation) or deemed critical to protecting CMS operations and assets, individuals, other organizations, and the Nation are assessed more frequently in accordance with an organizational assessment of risk. All other controls are assessed at least once during the information system's three-year authorization cycle. The organization can use the current year's assessment results from any of the above sources to meet the FISMA annual assessment requirement provided that the results are current, valid, and relevant to determining security control effectiveness. Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control.

CA-2 Compliance Description:

CA-2(1) - Independent Assessors – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs assessors or assessment teams with CMS CISO defined level of independence to conduct security control assessments.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.

Guidance
Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information systems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.

CA-2(1) Compliance Description:

CA-3 – System Interconnections

CMS ARS Mod 2.0 - Control:
The organization:
a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Reviews and updates the Interconnection Security Agreements on an ongoing basis verifying enforcement of security requirements.

Implementation Standard(s)
1. Record each system interconnection in the security plan for the system that is connected to the remote location.
2. The Interconnection Security Agreement or data sharing agreement is updated following significant changes to the system, organizations, or the nature of the electronic sharing of information that could impact the validity of the agreement.

Guidance
This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. The CMS authorizing official determines the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same CMS Business Owner, an Interconnection Security Agreement is not required. Instead, interface characteristics between the interconnecting information systems can be described in the security plans for their respective systems. If the interconnecting systems have different CMS Business Owners but the Business Owners are in the same organization, the organizations determine whether either a Memorandum of Understanding (MOU) and/or Service Level Agreement (SLA) is required. Instead of developing an Interconnection Security Agreement, organizations may choose to incorporate this information into formal contracts, especially if the interconnection is to be established between CMS and a nonfederal (private sector) organization. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls.

CA-3 Compliance Description:

CA-3(5) - Restrictions on External System Connections – Enhancement (Moderate) P1

CMS ARS Mod 2.0 - Control:
The organization employs, and documents in the applicable security plan, either i) allow-all, deny-by-exception, or, ii) deny-all, permit-by-exception (preferred), policy for allowing defined information systems (defined in the applicable security plan) to connect to external information systems.

Guidance
Organizations can constrain information system connectivity to external domains (e.g., websites) by employing one of two policies with regard to such connectivity: (i) allow-all, deny by exception, also known as blacklisting (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as whitelisting (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable.

CA-3(5) Compliance Description:

CA-5 – Plan of Action and Milestones (Moderate) Assurance - P3

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops and submits a plan of action and milestones for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., SCA, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates and submits existing plan of action and milestones monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Implementation Standard(s)

Guidance
Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB.

CA-5 Compliance Description:

CA-5(1) - Automation Support for Accuracy/Currency – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.

Guidance
None

CA-5(1) Compliance Description:

CA-6 – Security Authorization

CMS ARS Mod 2.0 - Control:
The organization:
a. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
b. Updates the security authorization:
- Within every three (3) years;
- When significant changes are made to the system;
- When changes in requirements result in the need to process data of a higher sensitivity;
- When changes occur to authorizing legislation or federal requirements;
- After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and
- Prior to expiration of a previous security authorization.

Guidance
Security authorizations are official management decisions, conveyed through authorization decision documents, by the CMS CIO or his/her designated representative (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to CMS operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Explicit authorization to operate the information system is provided by the CMS CIO or his/her designated representative prior to a system being placed into operations. Through the security authorization process, the CMS CIO is accountable for security risks associated with the operation and use of CMS information system.
OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing the CMS CIO and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, the CMS CIO uses results of the continuous monitoring processes to the maximum extent possible as the basis for rendering a reauthorization decisions.
(For CSP only) Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. The service provider describes the types of changes to the information system or the environment of operations that would require a reauthorization of the information system. The types of changes are approved and accepted by the Joint Authorization Board (JAB).

CA-6 Compliance Description:

CA-7 – Continuous Monitoring

CMS ARS Mod 2.0 - Control:
The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:
a. Establishment of defined metrics (defined in the applicable security plan) to be monitored;
b. Establishment of defined frequencies (defined in the applicable security plan) for monitoring and defined frequencies (defined in the applicable security plan) for assessments supporting such monitoring;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
e. Correlation and analysis of security-related information generated by assessments and monitoring;
f. Response actions to address results of the analysis of security-related information; and
g. Reporting the security status of organization and the information system to defined personnel or roles (defined in the applicable security plan) monthly.

Guidance
Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational riskbased decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems.

CA-7 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Incident Response (IR) Controls

IR-1 – Incident Response Policy and Procedures

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
b. Reviews and updates (as necessary) the current:
1. Incident response policy within every three hundred sixty-five (365) days; and
2. Incident response procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

IR-1 Compliance Description:

IR-2 – Incident Response Training

CMS ARS Mod 2.0 - Control:
The organization provides incident response training to information system users consistent with assigned roles and responsibilities:
a. Within ninety (90) days of assuming an incident response role or responsibility;
b. When required by information system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

Guidance
Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

IR-2 Compliance Description:

IR-3 – Incident Response Testing

CMS ARS Mod 2.0 - Control:
The organization tests the incident response capability for the information system within every three hundred sixty-five (365) days using NIST SP 800-61, reviews, analyses, and simulations to determine the incident response effectiveness and documents the results. A formal test need not be conducted if the organization actively exercises its response capability using real incidents.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended).
2. **(For CSP only)** For service providers, the organization provides test plans to FedRAMP annually. Test plans are approved and accepted by the Joint Authorization Board (JAB) prior to test commencing.

Guidance
Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

IR-3 Compliance Description:

IR-3(2) - Coordination with Related Plans – Enhancement

CMS ARS Mod 2.0 - Control:
The organization coordinates incident response testing with organizational elements responsible for related plans.

Guidance
Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

IR-3(2) Compliance Description:

IR-4 – Incident Handling

CMS ARS Mod 2.0 - Control:
The organization:
a. Implements an incident handling capability using the current Risk Management Handbook (RMH), Volume II, Procedure 7.2, Incident Handling;
b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Implementation Standard(s)
1. Document relevant information related to a security incident according to the current Risk Management Handbook (RMH), Volume II, Procedure 7.2, Incident Handling.
2. Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence.
3. Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure.
4. **(For CSP only)** For service providers, the organization ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

Guidance
Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).

IR-4 Compliance Description:

IR-4(1) - Automated Incident Handling Processes – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs automated mechanisms to support the incident handling process.

Guidance
Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

IR-4(1) Compliance Description:

IR-5 – Incident Monitoring

CMS ARS Mod 2.0 - Control:
The organization tracks and documents information system security incidents.

Guidance
Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

IR-5 Compliance Description:

IR-6 – Incident Reporting

CMS ARS Mod 2.0 - Control:
The organization:
a. Requires personnel to report suspected security incidents to the organizational incident response capability within the timeframe established in the current Risk Management Handbook (RMH), Volume II, Procedure 7.2, Incident Handling; and
b. Reports security incident information to designated authorities.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Control. The organization requires personnel to report suspected security incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended).

Guidance
The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.
For more information see the see the Risk Management Handbook (RMH), Volume III, Standard 7.1, Incident Handling and Breach Notification.

IR-6 Compliance Description:

IR-6(1) - Automated Reporting – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs automated mechanisms to assist in the reporting of security incidents.

Guidance
None

IR-6(1) Compliance Description:

IR-7 – Incident Response Assistance

CMS ARS Mod 2.0 - Control:
The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Guidance
Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. The CMS CISO is available for assistance at mailto:CISO@cms.hhs.gov.

IR-7 Compliance Description:

IR-7(1) - Automation Support for Availability of Information/Support – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Guidance
Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

IR-7(1) Compliance Description:

IR-7(2) - Coordination with External Providers – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the organization:
(a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and
(b) Identifies organizational incident response team members to the external providers.

Guidance
(For CSP only) External providers of information system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.

IR-7(2) Compliance Description:

IR-8 – Incident Response Plan

CMS ARS Mod 2.0 - Control:

The organization:

a. Develops an incident response plan that:
1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
8. Is reviewed and approved by the applicable Incident Response Team Leader;
b. Distributes copies of the incident response plan to:
- CMS Chief Information Security Officer;
- CMS Chief Information Officer;
- Information System Security Officer;
- CMS Office of the Inspector General/Computer Crimes Unit;
- All personnel within the organization Incident Response Team;
- All personnel within the PII Breach Response Team; and
- All personnel within the organization Operations Centers;
c. Reviews the incident response plan within every three hundred sixty-five (365) days;
d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
e. Communicates incident response plan changes to the organizational elements listed in b. above; and
f. Protects the incident response plan from unauthorized disclosure and modification.

Implementation Standard(s)

1. **(For CSP only)** For service providers, the organization defines a list of incident response personnel (identified by name and/or by role) and organizational elements to distribute the response plan to. The incident response list includes designated FedRAMP personnel.
2. **(For CSP only)** For service providers, the organization defines a list of incident response personnel (identified by name and/or by role) and organizational elements to communicate any changes to. The incident response

Guidance

It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems.

IR-8 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Planning (PL) Controls

PL-1 – Security Planning Policy and Procedures

CMS ARS Mod 2.0 Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
b. Reviews and updates (as necessary) the current:
1. Security planning policy within every three hundred sixty-five (365) days; and
2. Security planning procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

PL-1 Compliance Description:

PL-2 – System Security Plan

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops a security plan for the information system that is consistent with the Risk Management Handbook (RMH) Procedures; and
1. Is consistent with the organization's enterprise architecture;
2. Explicitly defines the authorization boundary for the system;
3. Describes the operational context of the information system in terms of missions and business processes;
4. Provides the security categorization of the information system including supporting rationale;
5. Describes the operational environment for the information system and relationships with or connections to other information systems;
6. Provides an overview of the security requirements for the system;
7. Identifies any relevant overlays, if applicable;
8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
b. Distributes copies of the security plan and communicates subsequent changes to the plan to stakeholders;
c. Reviews the security plan for the information system within every three hundred sixty-five (365) days; and
d. Updates the plan, minimally every three (3) years, to address current conditions or whenever:
- There are significant changes to the information system/environment of operation that affect security;
- Problems are identified during plan implementation or security control assessments;
- When the data sensitivity level increases;
- After a serious security violation due to changes in the threat environment; or
- Before the previous security authorization expires; and
e. Protects the security plan from unauthorized disclosure and modification.

Implementation Standard(s)
1. **(For PHI only)** Retain documentation of policies and procedures relating to HIPAA 164.306 for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b).)
2. **(For FTI only)** When FTI is incorporated into a Data Warehouse, the controls described in IRS Pub. 1075, Exhibit 11 are to be followed, in addition to those specified in other controls.
3. **(For FTI only)** Develop and submit a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the confidentiality of FTI, and finally, certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the

Guidance
Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in NIST 800-53 Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). NIST 800-53 Appendix I provides guidance on developing overlays.
Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans.

PL-2 Compliance Description:

PL-2(3) - Plan/Coordinate with Other Organizational Entities – Enhancement

CMS ARS Mod 2.0 - Control:
The organization plans and coordinates security-related activities affecting the information system with affected stakeholders before conducting such activities in order to reduce the impact on other organizational entities.

Guidance
Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or nonurgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate.

PL-2(3) Compliance Description:

PL-4 – Rules of Behavior

CMS ARS Mod 2.0 - Control:
The organization:
a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
b. Receives an acknowledgment (paper or electronic) from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
c. Reviews and updates the rules of behavior every three hundred sixty-five (365) days; and
d. Requires individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules of behavior are revised/updated.

Guidance
This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from federal information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b. (the acknowledgment portion of this control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures (or other electronic mechanisms) for acknowledging rules of behavior.
Rules of behavior are aligned with DHHS requirements posted at http://hhs.gov/ocio/policy/2008-0001.003s.html, and made readily available.

PL-4 Compliance Description:

PL-4(1) - Social Media and Networking Restrictions – Enhancement

CMS ARS Mod 2.0 - Control:
The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Guidance
This control enhancement addresses rules of behavior related to the use of social media/networking sites: (i) when organizational personnel are using such sites for official duties or in the conduct of official business; (ii) when organizational information is involved in social media/networking transactions; and (iii) when personnel are accessing social media/networking sites from organizational information systems. Organizations also address specific rules that prevent unauthorized entities from obtaining and/or inferring nonpublic organizational information (e.g., system account information, personally identifiable information) from social media/networking sites.

PL-4(1) Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Risk Assessment (RA) Controls

RA-1 – Risk Assessment Policy and Procedures

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls on information systems and paper records; and
b. Reviews and updates (as necessary) the current:
1. Risk assessment policy within every three hundred sixty-five (365) days; and
2. Risk assessment procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

RA-1 Compliance Description:

RA-2 – Security Categorization

CMS ARS Mod 2.0 - Control:
The organization:
a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Guidance
Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted.
All CMS information systems categorized as High or Moderate are considered sensitive or to contain sensitive information. All CMS information systems categorized as Low are considered non-sensitive or to contain non-sensitive information. Organizations implement the minimum security requirements and controls as established in the current CMS Information Security ARS Standard, based on the system security categorization.

RA-2 Compliance Description:

RA-3 – Risk Assessment

CMS ARS Mod 2.0 - Control:
The organization:
a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in the applicable security plan;
c. Reviews risk assessment results within every three hundred sixty-five (365) days;
d. Disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO; and
e. Updates the risk assessment before issuing a new ATO package or within every three (3) years, whichever comes first; or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization documents risk assessment results in the security assessment report.
2. **(For CSP only)** For service providers, the organization reviews risk assessment results at least every three (3) years or when a significant change occurs.

Guidance
Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems.
Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation.
(For CSP only) Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.

RA-3 Compliance Description:

RA-5 – Vulnerability Scanning

CMS ARS Mod 2.0 - Control:
The organization:
a. Scans for vulnerabilities in the information system and hosted applications within every thirty (30) days and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with affected/related stakeholders on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Implementation Standard(s)
1. Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once within every three hundred sixty-five (365) days, in accordance with CMS IS procedures.
2. **(For CSP only)** For service providers, the organization scans for vulnerabilities in the information system and hosted applications quarterly; and operating system, web application, and database scans (as applicable); and when new vulnerabilities potentially affecting the system/applications are identified and reported;
3. **(For CSP only)** For service providers, the organization remediates legitimate high-risk vulnerabilities mitigated within thirty (30) days, and moderate risk vulnerabilities mitigated with ninety (90) days.

Guidance
Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

RA-5 Compliance Description:

RA-5(1) - Update Tool Capability – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities scanned.

Guidance
The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible.

RA-5(1) Compliance Description:

RA-5(2) - Update by Frequency/Prior to New Scan/When Identified – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) The organization updates the information system vulnerabilities scanned within every thirty (30) days or when new vulnerabilities are identified and reported.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The organization updates the list of information system vulnerabilities scanned continuously, before each scan.

Guidance
None

RA-5(2) Compliance Description:

RA-5(3) - Breadth/Depth of Coverage – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

Guidance
None

RA-5(3) Compliance Description:

RA-5(5) - Privileged Access – Enhancement

CMS ARS Mod 2.0 - Control:
The information system implements privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning.

Guidance
In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.

RA-5(5) Compliance Description:

RA-5(6) - Automated Trend Analyses – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

Guidance
None

RA-5(6) Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Access Control (AC) Controls

AC-1 – Access Control Policy and Procedures

CMS ARS Mod 2.0 - Control
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
b. Reviews and updates (as necessary) the current:
1. Access control policy within every three hundred sixty-five (365) days; and
2. Access control procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

AC-1 Compliance Description:

AC-2 – Account Management

CMS ARS Mod 2.0 - Control
The organization:
a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group, system, application, guest/anonymous, emergency, and temporary;
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by defined personnel or roles (defined in the applicable security plan) for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with ARS requirements and Risk Management Handbook (RMH) Standards and Procedures;
g. Monitors the use of, information system accounts;
h. Notifies account managers:
1. When accounts are no longer required;
2. When users are terminated or transferred; and
3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements using the frequency specified in Implementation Standard 1; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Implementation Standard(s)
1. Review information system accounts for compliance with account management requirements within every one hundred eighty (180) days, and require annual certification of all accounts within every three hundred sixty-five (365) days.
2. Remove or disable default user accounts. Rename active default accounts.
3. Implement centralized control of user access administrator functions.
4. Regulate the access provided to contractors and define security requirements for contractors.
5. (For CSP only) For service providers, the organization reviews information system accounts and requires certification at least annually.

Guidance
Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training.

AC-2 Compliance Description:

AC-2(1) - Automated Information System Account Management – Enhancement

CMS ARS Mod 2.0 - Control
The organization employs automated mechanisms to support the management of information system accounts.

Guidance
The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using telephonic notification to report atypical information system account usage.

AC 2(1) Compliance Description:

AC-2(2) - Removal of Temporary/Emergency Accounts – Enhancement

CMS ARS Mod 2.0 - Control
The information system automatically disables emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed three hundred sixtyfive
(365) days.
Implementation Standard(s)
1. **(For CSP only)** For service providers, the information system automatically disables temporary and emergency account types after no more than ninety (90) days.
Guidance
This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.

Guidance
This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.

AC-2(2) Compliance Description:

AC-2(3) - Disable Inactive Accounts – Enhancement

CMS ARS Mod 2.0 - Control
The information system automatically disables inactive accounts within sixty (60) days.
Implementation Standard(s)
1. **(For CSP only)** For service providers, the information system automatically disables inactive accounts within sixty (60) days.
2. **(For CSP only)** For service providers, the organization defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the Joint Authorization Board (JAB).

Guidance
None

AC-2(3) Compliance Description:

AC-2(4) - Automated Audit Actions – Enhancement

CMS ARS Mod 2.0 - Control
The information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies defined personnel or roles (defined in the applicable security plan).

Guidance
None

AC-2(4) Compliance Description:

AC-2(7) - Role-Based Schemes – Enhancement

CMS ARS Mod 2.0 - Control
(For CSP only) The organization:
(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
(b) Monitors privileged role assignments; and
(c) Inspects administrator groups, root accounts and other system related accounts on demand, but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created.

Guidance
(For CSP only) Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.

AC-2(7) Compliance Description:

AC-3 Access Enforcement

CMS ARS Mod 2.0 - Control
The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
Implementation Standard(s)
1. If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13).
2. Configure operating system controls to disable public "read" and "write" access to files, objects, and directories that may directly impact system functionality and/or performance, or that contain sensitive information.
3. Data stored in the information system must be protected with system access controls.

Guidance
Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security.
For minimum authentication requirements, refer to Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards.

AC-3 Compliance Description:

AC-3(3) - Mandatory Access Control – Enhancement

CMS ARS Mod 2.0 - Control
(For CSP only) For service providers, the information system enforces role-based access control policies over all subjects and objects where the policy specifies that:
(a) The policy is uniformly enforced across all subjects and objects within the boundary of the information system;
(b) A subject that has been granted access to information is constrained from doing any of the following;
(1) Passing the information to unauthorized subjects or objects;
(2) Granting its privileges to other subjects;
(3) Changing one or more security attributes on subjects, objects, the information system, or information system components;
(4) Choosing the security attributes and attribute values to be associated with newly created or modified objects; or
(5) Changing the rules governing access control; and
(c) FedRAMP-defined subjects may explicitly be granted FedRAMP-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints.
Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization:
a. Assigns user accounts and authenticators in accordance within service provider's role-based access control policies;
b. Configures the information system to request user ID and authenticator prior to system access; and
c. Configures the databases containing federal information in accordance with service provider's security administration guide to provide role-based access controls enforcing assigned privileges and permissions at the file, table, row, column, or cell level, as appropriate.

Guidance
(For CSP only) Mandatory access control as defined in this control enhancement is synonymous with nondiscretionary access control, and is not constrained only to certain historical uses (e.g., implementations using the Bell-LaPadula Model). The above class of mandatory access control policies constrains what actions subjects can take with information obtained from data objects for which they have already been granted access, thus preventing the subjects from passing the information to unauthorized subjects and objects. This class of mandatory access control policies also constrains what actions subjects can take with respect to the propagation of access control privileges; that is, a subject with a privilege cannot pass that privilege to other subjects. The policy is uniformly enforced over all subjects and objects to which the information system has control. Otherwise, the access control policy can be circumvented. This enforcement typically is provided via an implementation that meets the reference monitor concept (see AC-25). The policy is bounded by the information system boundary (i.e., once the information is passed outside of the control of the system, additional means may be required to ensure that the constraints on the information remain in effect). The trusted subjects described above are granted privileges consistent with the concept of least privilege (see AC-6).
Trusted subjects are only given the minimum privileges relative to the above policy necessary for satisfying organizational mission/business needs. The control is most applicable when there is some policy mandate (e.g., law, Executive Order, directive, or regulation) that establishes a policy regarding access to sensitive/classified information and some users of the information system are not authorized access to all sensitive/classified information resident in the information system. This control can operate in conjunction with AC-3 (4). A subject that is constrained in its operation by policies governed by this control is still able to operate under the less rigorous constraints of AC-3 (4), but policies governed by this control take precedence over the less rigorous constraints of AC-3 (4). For example, while a mandatory access control policy imposes a constraint preventing a subject from passing information to another subject operating at a different sensitivity label, AC-3 (4) permits the subject to pass the information to any subject with the same sensitivity label as the subject.

AC-3(3) Compliance Description:

AC-4 - Information Flow Enforcement

CMS ARS Mod 2.0 - Control:
The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Guidance
Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels.
Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. NIST 800-53 control enhancements 3 through 22 primarily address crossdomain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products.

AC-4 Compliance Description:

AC-5 - Separation of Duties

CMS ARS Mod 2.0 - Control
The organization:
a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
b. Documents separation of duties; and
c. Defines information system access authorizations to support separation of duties.

Implementation Standard(s)
1. Ensure that audit functions are not performed by security personnel responsible for administering access control.
2. Maintain a limited group of administrators with access based upon the users' roles and responsibilities.
3. Ensure that critical mission functions and information system support functions are divided among separate individuals.
4. Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.
5. Ensure that an independent entity, not the Business Owner, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system.

Guidance
Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

AC-5 Compliance Description:

AC-6 - Least Privilege

CMS ARS Mod 2.0 - Control
The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with CMS missions and business functions.

Implementation Standard(s)
1. Disable all file system access not explicitly required for system, application, and administrator functionality.
2. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS security policy.
3. Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control.
4. Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.
5. Disable all system and removable media boot access unless it is explicitly authorized by the CIO for compelling operational needs. If system and removable media boot access is authorized, boot access is password protected.

Guidance
Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.

AC-6 Compliance Description:

AC-6(1) - Authorize Access to Security Functions – Enhancement

CMS ARS Mod 2.0 - Control
At a minimum, the organization explicitly authorizes access to the following list of security functions (deployed in hardware, software, and firmware) and security-relevant information:
- Setting/modifying audit logs and auditing behavior;
- Setting/modifying boundary protection system rules;
- Configuring/modifying access authorizations (i.e., permissions, privileges);
- Setting/modifying authentication parameters; and
- Setting/modifying system configurations and parameters.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization explicitly authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information.
2. **(For CSP only)** For service providers, the organization defines the list of security functions. The list of functions is approved and accepted by the Joint Authorization Board (JAB).

Guidance
Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.

AC-6(1) Compliance Description:

AC-6(2) - Non-Privileged Access for Nonsecurity Functions – Enhancement

CMS ARS Mod 2.0 - Control
At a minimum, the organization requires that users of information system accounts, or roles, with access to the following list of security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions:
- Setting/modifying audit logs and auditing behavior;
- Setting/modifying boundary protection system rules;
- Configuring/modifying access authorizations (i.e., permissions, privileges);
- Setting/modifying authentication parameters; and
- Setting/modifying system configurations and parameters.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization requires that users of information system accounts, or roles, with access to all security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.

Guidance
This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.
(For CSP only) Examples of service provider security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.

AC-6(2) Compliance Description:

AC-6(5) - Privileged Accounts – Enhancement

CMS ARS Mod 2.0 - Control
The organization restricts privileged accounts on the information system to defined personnel or roles (defined in the applicable security plan).

Guidance
Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.

AC-6(5) Compliance Description:

AC-6(9) - Auditing Use of Privileged Functions – Enhancement

CMS ARS Mod 2.0 - Control
The information system audits the execution of privileged functions.

Guidance
Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT).

AC-6(9) Compliance Description:

AC-6(10) - Prohibit Non-Privileged Users from Executing Privileged Functions – Enhancement

CMS ARS Mod 2.0 - Control
Control
The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Guidance
Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

AC-6(10) Compliance Description:

AC-7 – Unsuccessful Logon Attempts

CMS ARS Mod 2.0 - Control
The information system:
a. Enforces the limit of consecutive invalid login attempts by a user specified in Implementation Standard 1 during the time period specified in Implementation Standard 1; and
b. Automatically disables or locks the account/node until released by an administrator or after the time period specified in Implementation Standard 1 when the maximum number of unsuccessful attempts is exceeded.

Implementation Standard(s)
1. Configure the information system to lock out the user account automatically after three (3) invalid login attempts during a fifteen (15) minute time period. Require the lock out to persist for a minimum of one (1) hour.
2. **(For CSP only)** For service providers, the information system:
a. Enforces a limit of not more than three (3) consecutive invalid login attempts by a user during a fifteen (15) minute time period; and
b. Automatically locks the account/node for thirty (30) minutes when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

Guidance
This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels.

AC-7 Compliance Description:

AC-8 – System Use Notification

CMS ARS Mod 2.0 - Control
The information system:
a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The approved banner states:
- You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
* You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.
* Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.
b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and
c. For publicly accessible systems:
1. Displays system use information when appropriate, before granting further access;
2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Includes a description of the authorized uses of the system.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization determines elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the Joint Authorization Board (JAB).
2. **(For CSP only)** For service providers, the organization determines how System Use Notification is going to be verified and provides appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the Joint Authorization Board (JAB).
3. **(For CSP only)** For service providers, if not performed as part of a Configuration Baseline check, the organization has a documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the Joint Authorization Board (JAB).

Guidance
The warning banner language has very important legal implications for CMS and its information system resources. Should content need to be added to this banner, submit the modified warning banner language to the CMS CIO for review and approval prior to implementation. If an information system has character limitations related to the warning banner display, the CMS CIO can provide an abbreviated warning banner version. If this banner is inconsistent with any directives, policies, regulations, or standards, notify the CMS CIO immediately.
All information system computers and network devices under CMS control, prominently display the notice and consent banner immediately upon users' authentication to the system, including, but not limited to, web sites, web pages where substantial personal information from the public is collected, sftp, SSH, or other services accessed. System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist.
(For CSP only) If performed as part of the service provider Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can
be provided.

AC-8 Compliance Description:

AC-10 – Concurrent Session Control

CMS ARS Mod 2.0 - Control
The information system limits the number of concurrent sessions for each system account to one (1) session. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one (1) concurrent application/process session is documented in the security plan.

Guidance
Organizations may define the maximum number of concurrent sessions for information system accounts globally, by account type (e.g., privileged user, non-privileged user, domain, specific application), by account, or a combination. For example, organizations may limit the number of concurrent sessions for system administrators or individuals working in particularly sensitive domains or mission-critical applications. This control addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts.
A session is defined as 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. Some systems may require concurrent user sessions to function properly. However, based on the operational needs, automated mechanisms limit the number of concurrent user sessions. It is good practice to have management's approval for any system to have user concurrent sessions. Management should review the need for user concurrent sessions within every three hundred sixty-five (365) days.

AC-10 Compliance Description:

AC-11 Session Lock

CMS ARS Mod 2.0 - Control
The information system:
a. Prevents further access to the system by initiating a session lock after thirty (30) minutes of inactivity or upon receiving a request from a user; and
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Guidance
Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays.

AC-11 Compliance Description:

AC-11(1) - Pattern-Hiding Displays – Enhancement

CMS ARS Mod 2.0 - Control
The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Guidance
Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.
(For CSP only) IaaS and PaaS.

AC-11(1) Compliance Description:

AC-12 – Session Termination

CMS ARS Mod 2.0 - Control
The information system automatically terminates a user session after defined conditions or trigger events (defined in the applicable security plan) requiring session disconnect.

Guidance
This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use.

AC-12 Compliance Description:

AC-14 Permitted Actions without Identification or Authentication

CMS ARS Mod 2.0 - Control
The organization:
a. Identifies specific user actions that can be performed on the information system without identification or authentication;
b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication; and
c. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.

Guidance
This control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be none.

AC-14 Compliance Description:

AC-16 – Security Attributes

CMS ARS Mod 2.0 - Control
(For CSP only) For service providers, the organization:
a. Provides the means to associate FedRAMP-defined types of security attributes having FedRAMP-defined security attribute values, as approved and accepted by Joint Authorization Board (JAB), with information in storage, in process, and/or in transmission;
b. Ensures that the security attribute associations are made and retained with the information;
c. Establishes the permitted FedRAMP-defined security attributes for FedRAMP-defined information systems; and
d. Determines the permitted FedRAMP-defined values or ranges for each of the established security attributes.

Guidance
(For CSP only) Information is represented internally within information systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures such as records, buffers, tables, files, inter-process pipes, and communications ports. Security attributes, a form of metadata, are abstractions representing the basic properties or characteristics of active and passive entities with respect to safeguarding information. These attributes may be associated with active entities (i.e., subjects) that have the potential to send or receive information, to cause information to flow among objects, or to change the information system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of security attributes to subjects and objects is referred to as binding and is typically inclusive of setting the attribute value and the attribute type. Security attributes when bound to data/information, enables the enforcement of information security policies for access control and information flow control, either through organizational processes or information system functions or mechanisms. The content or assigned values of security attributes can directly affect the ability of individuals to access organizational information. Organizations can define the types of attributes needed for selected information systems to support missions/business functions. There is potentially a wide range of values that can be assigned to any given security attribute. Release markings could include, for example, US only, NATO, or NOFORN (not releasable to foreign nationals). By specifying permitted attribute ranges and values, organizations can ensure that the security attribute values are meaningful and relevant. The term security labeling refers to the association of security attributes with subjects and objects represented by internal data structures within organizational information systems, to enable information system-based enforcement of information security policies. Security labels include, for example, access authorizations, data life cycle protection (i.e., encryption and data expiration), nationality, affiliation as contractor, and classification of information in accordance with legal and compliance requirements. The term security marking refers to the association of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies. The AC-16 base control represents the requirement for user-based attribute association (marking). The enhancements to AC-16 represent additional requirements including information system-based attribute association (labeling). Types of attributes include, for example, classification level for objects and clearance (access authorization) level for subjects. An example of a value for both of these attribute types is Top Secret.

AC-16 Compliance Description:

AC-17 Remote Access

CMS ARS Mod 2.0 - Control
The organization monitors for unauthorized remote access to the information system. Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the CIO or his/her designated representative. If remote access is authorized, the organization:
a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorizes remote access to the information system prior to allowing such connections.

Implementation Standard(s)
1. Require callback capability with re-authentication to verify connections from authorized locations when the CMS Net or Multi Protocol Label Switching (MPLS) service network cannot be used.
2. All computers and devices, whether government-furnished equipment (GFE) or contractor-furnished equipment (CFE), that require any network access to a network or system are securely configured and meet at least the following security requirements: (i) up-to-date system patches, and (ii) current anti-virus software; and (iii) functionality that provides the capability for automatic execution of code disabled.

Guidance
Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs, does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. For minimum authentication requirements, refer to Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards.

AC-17 Compliance Description:

AC-17(1) - Automated Monitoring/Control – Enhancement

CMS ARS Mod 2.0 - Control
The information system monitors and controls remote access methods.

Guidance
Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

AC-17(1) Compliance Description:

AC-17(2) - Protection of Confidentiality/Integrity Using Encryption – Enhancement

CMS ARS Mod 2.0 - Control
The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Guidance
The encryption strength of mechanism is selected based on the security categorization of the information. Use only the CMS-approved encryption standard (see SC-13).

AC-17(2) Compliance Description:

AC-17AC-17(3) - Managed Access Control Points – Enhancement

CMS ARS Mod 2.0 - Control
The information system routes all remote accesses through a limited number of managed access control points.

Guidance
Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections.

AC-17(3) Compliance Description:

AC-17(4) - Privileged Commands/Access – Enhancement

CMS ARS Mod 2.0 - Control
The organization:
(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs; and
(b) Documents the rationale for such access in the security plan for the information system.

Guidance
None

AC-17(4) Compliance Description:

AC-18 – Wireless Access

CMS ARS Mod 2.0 - Control
The organization monitors for unauthorized wireless access to information systems and prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If wireless access is authorized, the organization establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access prior to allowing such connections.

Implementation Standard(s)
1. If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless restrictions and access controls are implemented:
(a) Encryption protection is enabled;
(b) Access points are placed in secure areas;
(c) Access points are shut down when not in use (i.e., nights, weekends);
(d) A firewall is implemented between the wireless network and the wired infrastructure;
(e) MAC address authentication is utilized;
(f) Static IP addresses, not DHCP, is utilized;
(g) Personal firewalls are utilized on all wireless clients;
(h) File sharing is disabled on all wireless clients;
(i) Intrusion detection agents are deployed on the wireless side of the firewall;
(j) Wireless activity is monitored and recorded, and the records are reviewed on a regular basis; and
(k) Adheres to CMS-CIO-POL-INF12-01, CMS Policy for Wireless Client Access.

Guidance
Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication.

AC-18 Compliance Description:

AC-18(1) - Authentication and Encryption – Enhancement

CMS ARS Mod 2.0 - Control
If wireless access is explicitly approved, the information system protects wireless access to the system using encryption, and authentication of both users and devices.

Guidance
None

AC-18(1) Compliance Description:

AC-19 – Access Control for Mobile Devices

CMS ARS Mod 2.0 - Control
The organization:
a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. CIO authorizes the connection of mobile devices to organizational information systems.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization defines inspection and preventative measures. The measures are approved and accepted by Joint Authorization Board (JAB).

Guidance
A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled.

AC-19 Compliance Description:

AC-19(5) - Full Device/Container-Based Encryption – Enhancement

CMS ARS Mod 2.0 - Control
The organization employs full-device encryption, or container encryption, to protect the confidentiality and integrity of information on approved mobile devices.

Guidance
Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields.

AC-19(5) Compliance Description:

AC-20 Use of External Information Systems

CMS ARS Mod 2.0 - Control
The organization prohibits the use of 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 to store, access, transmit, or process sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If external information systems are authorized, the organization establishes strict terms and conditions for their use.
The terms and conditions shall address, at a minimum:
a. The types of applications that can be accessed from external information systems;
b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
c. How other users of the external information system will be prevented from accessing federal information;
d. The use of virtual private networking (VPN) and firewall technologies;
e. The use of and protection against the vulnerabilities of wireless technologies;
f. The maintenance of adequate physical security controls;
g. The use of virus and spyware protection software; and
h. How often the security capabilities of installed software are to be updated.

Implementation Standard(s)
1. Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees.
2. **(For PII only)** Only organization owned computers and software can be used to process, access, and store PII.

Guidance
External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems. For some external information systems (i.e., information systems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments. This control does not apply to the use of external information systems to access public interfaces to organizational information systems (e.g., individuals accessing federal information through www.medicare.gov). Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: types of applications that can be accessed on organizational information systems from external information systems; and the highest security category of information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.
For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to CMS, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external.

AC-20 Compliance Description:

AC-20(1) - Limits on Authorized Use – Enhancement

CMS ARS Mod 2.0 - Control
The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
(a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
(b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

Guidance
This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

AC-20(1) Compliance Description:

AC-20(2) - Portable Storage Devices – Enhancement

CMS ARS Mod 2.0 - Control
The organization restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems.

Guidance
Limits on the use of organization-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

AC-20(2) Compliance Description:

AC-21 – Information Sharing

CMS ARS Mod 2.0 - Control
The organization:
a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for approved information-sharing circumstances where user discretion is required; and
b. Employs defined automated mechanisms, or manual processes, (defined in the applicable security plan) to assist users in making information sharing/collaboration decisions.

Guidance
This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment.

AC-21 Compliance Description:

AC-22 Publicly Accessible Content

CMS ARS Mod 2.0 - Control
The organization:
a. Designates individuals authorized to post information onto a publicly accessible information system;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
d. Reviews the content on the publicly accessible information system for nonpublic information bi-weekly and removes such information, if discovered.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization reviews the content on the publicly accessible organizational information system for nonpublic information at least quarterly.
Guidance
In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-CMS information systems is covered by organizational policy.

Guidance
In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-CMS information systems is covered by organizational policy.

AC-22 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Security Awareness and Training (AT) Controls

AT-1 – Security Awareness and Training Policy and Procedures

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A security and privacy awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security and privacy awareness and training policy and associated security and privacy awareness and training controls; and
b. Reviews and updates (as necessary) the current:
1. Security and privacy awareness and training policy within every three hundred sixty-five (365) days; and
2. Security and privacy awareness and training procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

AT-1 Compliance Description:

AT-2 – Security Awareness Training

CMS ARS Mod 2.0 - Control:
The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
a. As part of initial training for new users prior to accessing any system's information;
b. When required by system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

Implementation Standard(s)
1. An information security and privacy education and awareness training program is developed and implemented for all employees and individuals working on behalf of CMS involved in managing, using, and/or operating information systems.
2. Privacy awareness training is provided before granting access to systems and networks, and within every three hundred sixty-five (365) days thereafter, to all employees and contractors, to explain the importance and responsibility in safeguarding PII and ensuring privacy, as established in Federal legislation and OMB guidance.

Guidance
Organizations determine the appropriate content of security and privacy awareness training, and security and privacy awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and privacy, and to respond to suspected security and privacy incidents. The content also addresses awareness of the need for operations security and privacy as it relates to CMS' information security program. Security and privacy awareness techniques can include, for example, displaying posters, offering supplies inscribed with security and privacy reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security and privacy awareness events.

AT-2 Compliance Description:

AT-2(2) - Insider Threat – Enhancement

CMS ARS Mod 2.0 - Control:
The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Guidance
Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.

AT-2(2) Compliance Description:

AT-3 – Role-Based Security Training

CMS ARS Mod 2.0 - Control:
The organization provides role-based security training to personnel with assigned security roles and responsibilities:
a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

Implementation Standard(s)
1. Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to networks, systems, and/or applications; when required by significant information system or system environment changes; when an employee enters a new position that requires additional role-specific training; and refresher training within every three hundred sixty-five (365) days thereafter.
2. **(For CSP only)** For service providers, the organization provides refresher training a least every three (3) years thereafter.

Guidance
Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of CMS and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of CMS' information security programs. Role-based security training also applies to contractors providing services to federal agencies.

AT-3 Compliance Description:

AT-4 – Security Training Records (Moderate) Assurance - P3

CMS ARS Mod 2.0 - Control:
The organization:
a. Documents and monitors individual information system security and privacy training activities including basic security and privacy awareness training and specific information system security and privacy training; and
b. Retains individual training records for a minimum of five (5) years.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization retains individual training records for at least three (3) years.

Guidance

Procedures and training implementation should:

(a) Identify employees with significant information security and privacy responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:

1) All users of CMS information systems must be exposed to security and privacy awareness materials at least every 365 days. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.

2) Executives must receive training in information security and privacy basics and policy level training in security and privacy planning and management.

3) Program and functional managers must receive training in information security and privacy basics; management and implementation level training in security and privacy planning and system/application security and privacy management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.

4) Chief Information Officers (CIOs), information security and privacy program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security and privacy officers) must receive training in information security and privacy basics and broad training in security and privacy planning, system and application security and privacy management, system/application life cycle management, risk management, and contingency planning.

5) IT function management and operations personnel must receive training in information security and privacy basics; management and implementation level training in security and privacy planning and system/application security and privacy management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.

(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on information security awareness and training to all new employees before allowing them access to the systems.

(c) Provide information systems security and privacy refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.

(d) Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

Documentation for specialized training may be maintained by individual supervisors at the option of the organization.

AT-4 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Configuration Management (CM) Controls

CM-1 – Configuration Management Policy and Procedures

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
b. Reviews and updates (as necesssary) the current:
1. Configuration management policy within every three hundred sixty-five (365) days; and
2. Configuration management procedures within every three hundred sixty-five (365) days.

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

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

CM-1 Compliance Description:

CM-2 – Baseline Configuration

CMS ARS Mod 2.0 - Control:
The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Guidance
This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.

CM-2 Compliance Description:

CM-2(1) - Reviews and Updates – Enhancement (Moderate) Assurance - P1

CMS ARS Mod 2.0 - Control:
The organization reviews and updates the baseline configuration of the information system:
(a) At least every three hundred sixty-five (365) days;
(b) When configuration settings change due to critical security patches (as defined by the Federal Government, CMS, or vendor), upgrades and emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware components), major system changes/upgrades;
(c) (1) As an integral part of information system component installations, (2) upgrades, and (3) updates to applicable governing standards (implemented within timeline defined in
(a) above); and
(d) Supporting baseline configuration documentation reflects ongoing implementation of operational configuration baseline updates, either directly or by policy.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization reviews and updates the baseline configuration of the information system:
(a) Annually;
(b) When required due to a significant change; and
(c) As an integral part of information system component installations and upgrades.

Guidance
None.

CM-2(1) Compliance Description:

CM-2(3) - Retention of Previous Configurations – Enhancement

CMS ARS Mod 2.0 - Control:
The organization retains older versions of baseline configurations of the information system as deemed necessary to support rollback.

Guidance
Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.

CM-2(3) Compliance Description:

CM-2(7) - Configure Systems, Components, or Devices for High-Risk Areas – Enhancement

CMS ARS Mod 2.0 - Control:
The organization:
(a) Issues dedicated information systems, system components, or devices with stringent configurations to individuals traveling to locations that the organization deems to be of significant risk; and
(b) Applies detailed inspection or re-imaging of the devices when the individuals return.

Guidance
When it is known that information systems, system components, or devices (e.g., notebook computers, mobile devices) will be located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to organizational-controlled areas. For example, organizational policies and procedures for notebook computers used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the device after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

CM-2(7) Compliance Description:

CM-3 – Configuration Change Control

CMS ARS Mod 2.0 - Control:
The organization:
a. Determines the types of changes to the information system that are configuration-controlled;
b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
c. Documents configuration change decisions associated with the information system;
d. Implements approved configuration-controlled changes to the information system;
e. Retains records of configuration-controlled changes to the information system for at least three (3) years;
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
g. Coordinates and provides oversight for configuration change control activities through change request forms which must be approved by an organizational and/or CMS change control board that convenes frequently enough to accommodate proposed change requests, and other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization coordinates and provides oversight for configuration change control activities through organization-defined configuration change control element (e.g., committee, board] that convenes organization-defined frequency; organization-defined configuration change conditions.
2. **(For CSP only)** For service providers, the organization defines the configuration change control element and the frequency or conditions under which it is convened. The change control element and frequency/conditions of use are approved and accepted by the Joint Authorization Board (JAB).
3. **(For CSP only)** For service providers, the organization establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the Joint Authorization Board (JAB).

Guidance
Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes.

CM-3 Compliance Description:

CM-3(2) - Test/Validate/Document Changes – Enhancement

CMS ARS Mod 2.0 - Control:
The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

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

CM-3(2) Compliance Description:

CM-4 – Security Impact Analysis

CMS ARS Mod 2.0 - Control:
The organization analyzes changes to the information system to determine potential security and privacy impacts prior to change implementation. Activities associated with configuration changes to the information system are audited.

Guidance
Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems.

CM-4 Compliance Description:

CM-4(1) - Separate Test Environments – Enhancement

CMS ARS Mod 2.0 - Control:
The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Guidance
Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines).

CM-4(1) Compliance Description:

CM-4(2) - Verification of Security Functions – Enhancement

CMS ARS Mod 2.0 - Control:
The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

Guidance
Implementation in this context refers to installing changed code in the operational information system.

CM-4(2) Compliance Description:

CM-5 – Access Restrictions for Change

CMS ARS Mod 2.0 - Control:
The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.

Guidance
Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

CM-5 Compliance Description:

CM-5(1) - Automated Access Enforcement/Auditing – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) The information system enforces access restrictions and supports auditing of the enforcement actions.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

Guidance
None

CM-5(1) Compliance Description:

CM-5(5) - Limit Production/Operational Privileges – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the organization:
(a) Limits privileges to change information system components and system-related information within a production or operational environment; and
(b) Reviews and reevaluates privileges at least quarterly.

Guidance
(For CSP only) In many organizations, information systems support multiple core missions/business functions. Limiting privileges to change information system components with respect to operational systems is necessary because changes to a particular information system component may have far-reaching effects on mission/business processes supported by the system where the component resides. The complex, many-to-many relationships between systems and mission/business processes are in some cases, unknown to developers.

CM-5(5) Compliance Description:

CM-6 – Configuration Settings

CMS ARS Mod 2.0 - Control:
The organization:
a. Establishes and documents configuration settings for information technology products employed within the information system using the latest security configuration baselines established by the HHS, U.S. Government Configuration Baselines (USGCB), and the National Checklist Program (NCP) defined by NIST SP 800-70 Rev. 2 (refer to Implementation Standard 1 for specifics) that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for individual components within the information system based on explicit operational requirements; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Implementation Standard(s)
1. (a) HHS-specific minimum security configurations shall be used for the following Operating System (OS) and Applications:
- HHS FDCC Windows XP Standard
- HHS FDCC Windows Vista Standard
- Blackberry Server
- Websense.
(b) For all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing security configuration guidelines is as follows:
(1) USGCB
(2) NIST National Checklist Program (NCP); Tier IV, then Tier III, Tier II, and Tier I, in descending order.
(3) Defense Information Systems Agency (DISA) STIGs
(4) National Security Agency (NSA) STIGs
(5) If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group (such as The Center for Internet Security [CIS]) checklists.
(6) In situations where no guidance exists, coordinate with CMS for guidance. CMS shall collaborate within CMS and the HHS Cybersecurity Program, and other OPDIVs through the HHS Continuous Monitoring and Risk Scoring (CMRS) working group to establish baselines and communicate industry and vendor best practices.
(7) All deviations from existing USGCB, NCP, DISA and/or NSA configurations must be documented in an approved HHS waiver (available at http://intranet.hhs.gov/it/cybersecurity/policies_by_document_type/index.html#Policy and Standard Waiver), with copies submitted to the Department.
2. **(For CSP only)** For service providers, the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using United States Government Configuration Baseline (USGCB) that reflect the most restrictive mode consistent with operational requirements.
3. **(For CSP only)** For service providers, the organization shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establish own configuration settings if USGCB is not available. Configuration settings are approved and accepted by the Joint Authorization Board (JAB).
4. **(For CSP only)** For service providers, the organization ensures that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).

Guidance
Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline.
Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems.
(For CSP only) Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc.

CM-6 Compliance Description:

CM-6(1) - Automated Central Management/Application/Verification – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for FedRAMP-defined information system components.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

Guidance

CM-6(1) Compliance Description:

CM-7 – Least Functionality

CMS ARS Mod 2.0 - Control:
The organization:
a. Configures the information system to provide only essential capabilities; and
b. Prohibits or restricts the use of high-risk system services, ports, network protocols, and capabilities (e.g., Telnet FTP, etc.) across network boundaries that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the applicable security plan; all others will be disabled.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Control. The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: United States Government Configuration Baseline (USGCB)-defined list of prohibited or restricted functions, ports, protocols, and/or services.
2. **(For CSP only)** For service providers, the organization shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. The list of prohibited or restricted functions, ports, protocols, and/or services are approved and accepted by the Joint Authorization Board (JAB).

Guidance
Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing).
Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.
(For CSP only) Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc.

CM-7 Compliance Description:

CM-7(1) - Periodic Review – Enhancement

CMS ARS Mod 2.0 - Control:
The organization:
(a) Reviews the information system within every three hundred sixty-five (365) days to identify and eliminate unnecessary functions, ports, protocols, and/or services; and
(b) Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The organization reviews the information system at least quarterly to identify and eliminate unnecessary functions, ports, protocols, and/or services.

Guidance
The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols.

CM-7(1) Compliance Description:

CM-7(2) - Prevent Program Execution – Enhancement

CMS ARS Mod 2.0 - Control:
The information system prevents program execution in accordance with the list of authorized or unauthorized software programs and rules authorizing the terms and conditions of software program usage.

Guidance
None

CM-7(2) Compliance Description:

CM-7(4) - Unauthorized Software/Blacklisting – Enhancement

CMS ARS Mod 2.0 - Control:
The organization:
(a) Identifies defined software programs (defined in the applicable security plan) not authorized to execute on the information system;
(b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and
(c) Reviews and updates the list of unauthorized software programs within every three hundred sixty-five (365) days.

Guidance
The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as blacklisting. Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution.

CM-7(4) Compliance Description:

CM-8 – Information System Component Inventory

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops and documents an inventory of information system components that:
1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes:
- Unique identifier and/or serial number;
- Information system of which the component is a part;
- Type of information system component (e.g., server, desktop, application);
- Manufacturer/model information;
- Operating system type and version/service pack Level;
- Presence of virtual machines;
- Application software version/license information;
- Physical location (e.g., building/room number);
- Logical location (e.g., IP address, position with the IS architecture);
- Media access control (MAC) address;
- Ownership;
- Operational status;
- Primary and secondary administrators;
- Primary user; and
b. Reviews and updates the information system component inventory no less than every three hundred sixty-five (365) days, or per CM-8(1) and/or CM-8(2), as applicable.

Implementation Standard(s)
1. All Government-owned equipment (i.e., servers, workstations, laptops, and other IT components) used to process, store, or transmit CMS information display an asset tag with a unique identifying asset number. IT components with an asset tag are tracked in an asset inventory database to include (at a minimum) name, location, asset identification, owner, and description of use.
2. **(For CSP only)** For service providers, the organization develops, documents, and maintains an inventory of information system components that includes organization-defined information deemed necessary to achieve effective property accountability.
3. **(For CSP only)** For service providers, the organization defines information deemed necessary to achieve effective property accountability. Property accountability information are approved and accepted by the Joint Authorization Board (JAB).

Guidance
Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.
(For CSP only) Information deemed necessary to achieve effective property accountability may include hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address.

CM-8 Compliance Description:

CM-8(1) - Updates During Installations/Removals – Enhancement

CMS ARS Mod 2.0 - Control:
The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

Guidance
None

CM-8(1) Compliance Description:

CM-8(3) - Automated Unauthorized Component Detection – Enhancement

CMS ARS Mod 2.0 - Control:
The organization:
(a) Employs automated mechanisms to scan the network no less than weekly to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
(b) Takes the following actions when unauthorized components are detected: disables network access by such components/devices and notifies defined personnel or roles (defined in the applicable security plan).

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The organization:
(a) Employs automated mechanisms to scan continuously, using automated mechanisms with a maximum five-minute delay in detection to detect the addition of unauthorized components/devices into the information system; and
(b) Disables network access by such components/devices or notifies designated organizational officials.

Guidance
This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing.

CM-8(3) Compliance Description:

CM-8(5) - No Duplicate Accounting of Components – Enhancement

CMS ARS Mod 2.0 - Control:
The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

Guidance
This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.

CM-8(5) Compliance Description:

CM-9 – Configuration Management Plan

CMS ARS Mod 2.0 - Control:
The organization develops, documents, and implements a configuration management plan for the information system that:
a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the information system and places the configuration items under configuration management; and
d. Protects the configuration management plan from unauthorized disclosure and modification.

Guidance
Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control.

CM-9 Compliance Description:

CM-10 – Software Usage Restrictions

CMS ARS Mod 2.0 - Control:
The organization:
a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Guidance
Software license tracing can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.

CM-10 Compliance Description:

CM-11 – User-Installed Software

CMS ARS Mod 2.0 - Control:
The organization:
a. Establishes organization-defined policies governing the installation of software by users;
b. Enforces software installation policies through organization-defined methods; and
c. Monitors policy compliance at organization-defined frequency.

Guidance
If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved “app stores.” Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organizationdeveloped or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.

CM-11 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Identification and Authentication (IA) Controls

IA-1 – Identification and Authentication Policy and Procedures

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
b. Reviews and updates (as necessary) the current:
1. Identification and authentication policy within every three hundred sixty-five (365) days; and
2. Identification and authentication procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

IA-1 Compliance Description:

IA-2 – Identification and Authentication (Organizational Users)

CMS ARS Mod 2.0 - Control:
The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Implementation Standard(s)
1. Require the use of system and/or network authenticators and unique user identifiers.
2. Help desk support requires user identification for any transaction that has information security implications.

Guidance
Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.
Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8.

IA-2 Compliance Description:

IA-2(1) - Network Access to Privileged Accounts – Enhancement

CMS ARS Mod 2.0 - Control:
The information system implements multifactor authentication for network access to privileged accounts.

Guidance
None

IA-2(1) Compliance Description:

IA-2(2) - Network Access to Non-Privileged Accounts – Enhancement

CMS ARS Mod 2.0 - Control:
The information system implements multifactor authentication for network access to non-privileged accounts.

Guidance
None

IA-2(2) Compliance Description:

IA-2(3) - Local Access to Privileged Accounts – Enhancement

CMS ARS Mod 2.0 - Control:
The information system implements multifactor authentication for local access to privileged accounts.

Guidance
None

IA-2(3) Compliance Description:

IA-2(8) - Network Access to Privileged Accounts - Replay Resistant – Enhancement

CMS ARS Mod 2.0 - Control:
The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The organization defines replay-resistant authentication mechanisms. The mechanisms are approved and accepted by the Joint Authorization Board (JAB).

Guidance
Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

IA-2(8) Compliance Description:

IA-2(11) - Remote Access - Separate Device – Enhancement

CMS ARS Mod 2.0 - Control:
The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets minimum token requirements discussed in the Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards.

Guidance
For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users.

IA-2(11) Compliance Description:

IA-2(12) - Acceptance of PIV Credentials – Enhancement

CMS ARS Mod 2.0 - Control:
The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

Guidance
This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.

IA-2(12) Compliance Description:

IA-3 – Device Identification and Authentication

CMS ARS Mod 2.0 - Control:
The information system uniquely identifies and authenticates defined types of devices (defined in the applicable security plan) that require authentication mechanisms before establishing a connection that, at a minimum, use shared information (i.e., MAC or IP address) and access control lists to control remote network access.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Control. The organization defines a list a specific devices and/or types of devices. The list of devices and/or device types is approved and accepted by the Joint Authorization Board (JAB).

Guidance
Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability.
Note: At a minimum, CMS information systems should be filtered by MAC and/or IP address when accessing remote systems.

IA-3 Compliance Description:

IA-4 – Identifier Management

CMS ARS Mod 2.0 - Control:
The organization manages information system identifiers by:
a. Receiving authorization from defined personnel or roles (defined in the applicable security plan) to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group, role, or device;
d. Preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least three (3) years has expired; and
e. Disabling the identifier after sixty (60) days or less of inactivity and deleting disabled accounts during the annual re-certification process.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization prevents reuse of user or device identifiers for at least two (2) years and disables the user identifier after ninety (90) days of inactivity.
2. **(For CSP only)** For service providers, the organization defines time period of inactivity for device identifiers. The time period is approved and accepted by Joint Authorization Board (JAB).

Guidance
Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

IA-4 Compliance Description:

IA-4(4) - Identify User Status – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the organization manages individual identifiers by uniquely identifying each individual as contractors; foreign nationals.

Guidance
(For CSP only) Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.

IA-4(4) Compliance Description:

IA-5 – Authenticator Management

CMS ARS Mod 2.0 - Control:
Non-standard account-authenticator management specifications are addressed in the CMS Risk Management Handbook (RMH), Volume III, Standard 4.3, “Non-Standard Authenticator Management”. For all others, the organization manages information system authenticators by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators as follows:
- Passwords are valid for no longer than the period directed in IA-5(1);
- PIV compliant access cards are valid for no longer than five (5) years; and
- PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three (3) years;
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts changes.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization manages information system authenticators for users and devices by changing/refreshing authenticators every sixty (60) days by authenticator type.

Guidance
Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous onetime tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.

IA-5 Compliance Description:

IA-5(1) - Password-Based Authentication – Enhancement

CMS ARS Mod 2.0 - Control:
Non-standard account-authenticator management specifications are addressed in the CMS Risk Management Handbook (RMH), Volume III, Standard 4.3, “Non-Standard Authenticator Management”. For all other password-based authentication, the information systems follow the direction in the applicable configuration baselines per CM-6, or as follows, whichever is more stringent:
a. Prohibits the use of dictionary names or words;
b. Enforces at least the following minimum password requirements (User/Privileged/Process [acting on behalf of a User]):
- MinimumPasswordAge = 1/1/1;
- MaximumPasswordAge = 60/60/120;
- MinimumPasswordLength = 8/8/15;
- PasswordComplexity = minimum (1/1/3) character from the four (4) character categories (A-Z, a-z, 0-9, special characters; and
- PasswordHistorySize = 6/6/12;
c. If the operating environment allows, enforces a minimum of (4/4/8) changed characters when new passwords are created;
d. Stores and transmits only encrypted representations of passwords; and
e. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The information system, for password-based authentication:
(a) Enforces minimum password complexity of case sensitive, minimum of twelve (12) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters;
(b) Enforces at least one (1) changed character or as determined by the information system (where possible) when new passwords are created;
(c) Encrypts passwords in storage and in transmission;
(d) Enforces password minimum and maximum lifetime restrictions of one (1) day minimum, sixty (60) days maximum; and
(e) Prohibits password reuse for twenty four (24) generations.

Guidance
This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords.
(For CSP only) Mobile devices are excluded from the password complexity requirement.

IA-5(1) Compliance Description:

IA-5(2) - PKI-Based Authentication – Enhancement

CMS ARS Mod 2.0 - Control:
The information system, for PKI-based authentication:
(a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
(b) Enforces authorized access to the corresponding private key;
(c) Maps the authenticated identity to the account of the individual or group; and
(d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Guidance
Guidance
Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses. For PIV cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor including certificate policy processing.

IA-5(2) Compliance Description:

IA-5(3) - In-Person or Trusted Third-Party Registration – Enhancement

CMS ARS Mod 2.0 - Control:
The organization requires that the registration process to receive hardware administrative tokens and credentials used for two (2)-factor authentication be conducted in person before a designated registration authority with authorization by defined personnel or roles (defined in the applicable security plan).

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization requires that the registration process to receive HSPD-12 smart cards be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

Guidance
None

IA-5(3) Compliance Description:

IA-5(6) - Protection of Authenticators – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Guidance
(For CSP only) For information systems containing multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems.

IA-5(6) Compliance Description:

IA-5(7) - No Embedded Unencrypted Static Authenticators – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

Guidance
(For CSP only) Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

IA-2(11) Compliance Description:

IA-5(11) - Hardware Token-Based Authentication – Enhancement

CMS ARS Mod 2.0 - Control:
The information system, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements discussed in the Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards.

Guidance
Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular PKI.

IA-5(11) Compliance Description:

IA-6 Authenticator FeedbackIA-6 – Authenticator Feedback

CMS ARS Mod 2.0 - Control:
The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Guidance
The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

IA-6 Compliance Description:

IA-7 – Cryptographic Module Authentication

CMS ARS Mod 2.0 - Control:
The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Guidance
Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

IA-7 Compliance Description:

IA-8 – Identification and Authentication (Non-Organizational Users)

CMS ARS Mod 2.0 - Control:
The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Guidance
Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of nonorganizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users.
If E-Authentication is used, refer to Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards.

IA-8 Compliance Description:

IA-8(1) - Acceptance of PIV Credentials from Other Agencies – Enhancement

CMS ARS Mod 2.0 - Control:
The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

Guidance
This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.

IA-8(1) Compliance Description:

IA-8(2) - Acceptance of Third-Party Credentials – Enhancement

CMS ARS Mod 2.0 - Control:
The information system accepts only FICAM-approved third-party credentials.

Guidance
This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels.

IA-8(2) Compliance Description:

IA-8(3) - Use of FICAM-Approved Products – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs only FICAM-approved information system components in information systems that authenticate non-organizational users and accept third-party credentials.

Guidance
This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program.

IA-8(3) Compliance Description:

IA-8(4) - Use of FICAM-Issued Profiles – Enhancement

CMS ARS Mod 2.0 - Control:
The information system conforms to FICAM-issued profiles.

Guidance
This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange).

IA-8(4) Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Personnel Security (PS) Controls

PS-1 – Personnel Security Policy and Procedures

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
b. Reviews and updates (as necessary) the current:
1. Personnel security policy within every three hundred sixty-five (365) days; and
2. Personnel security procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

PS-1 Compliance Description:

PS-2 – Position Risk Designation

CMS ARS Mod 2.0 - Control:
The organization:
a. Assigns a risk designation to all organizational positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and revises position risk designations within every three hundred sixty-five (365) days.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization reviews and revises position risk designations at least every three (3) years.

Guidance
Position risk designations reflect Office of Personnel Management policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances).

PS-2 Compliance Description:

PS-3 – Personnel Screening

CMS ARS Mod 2.0 - Control:
The organization:
a. Screens individuals prior to authorizing access to the information system;
b. Rescreens individuals periodically, consistent with the risk designation of the position; and
c. When an employee moves from one position to another, the higher level of clearance should be adjudicated.

Implementation Standard(s)
1. Require that individuals with significant security responsibilities be assigned and hold, at a minimum, a Level 5 Public Trust sensitivity level clearance as defined in the HHS Personnel Security/Suitability Handbook. Assign other individuals with Public Trust positions the appropriate sensitivity level as defined in the HHS Personnel Security/Suitability Handbook.
2. **(For CSP only)** For service providers, this Standard replaces the above Control and Standard. The organization rescreens individuals according to following:
(a) For national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance.
(b) For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions.

Guidance
Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.

PS-3 Compliance Description:

PS-4 – Personnel Termination

CMS ARS Mod 2.0 - Control:
The organization, upon termination of individual employment:
a. Disables information system access in accordance with Implementation Standard 1;
b. Terminates/revokes any authenticators/credentials associated with the individual;
c. Conducts exit interviews that include a discussion of non-disclosure of information security and privacy information;
d. Retrieves all security-related organizational information system-related property;
e. Retains access to organizational information and information systems formerly controlled by terminated individual;
f. Notifies defined personnel or roles (defined in the applicable security plan) within one (1) business day; and
g. Immediately escorts employees terminated for cause out of the organization.

Implementation Standard(s)
1. System access must be revoked prior to or during the employee termination process.
2. All access and privileges to systems, networks, and facilities are suspended when employees or contractors temporarily separate from the organization (e.g., leave of absence).

Guidance
Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and nonavailability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Appropriate personnel have access to official records created by terminated employees that are stored on information systems.

PS-4 Compliance Description:

PS-5 – Personnel Transfer

CMS ARS Mod 2.0 - Control:
The organization:
a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiates the following transfer or reassignment actions during the formal transfer process:
(i). Re-issuing appropriate information system-related property (e.g., keys, identification cards, building passes);
(ii). Notification to security management;
(iii). Closing obsolete accounts and establishing new accounts;
(iv). When an employee moves to a new position of trust, logical and physical access controls must be re-evaluated as soon as possible but not to exceed thirty (30) days;
c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notifies defined personnel or roles (defined in the applicable security plan) within one (1) business day.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates organization-defined transfer or reassignment actions within five (5) days following the formal transfer action.
2. **(For CSP only)** For service providers, the organization defines transfer or reassignment actions. Transfer or reassignment actions are approved and accepted by the JAB.

Guidance
This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts.

PS-5 Compliance Description:

PS-6 – Access Agreements

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops and documents access agreements for organizational information systems;
b. Reviews and updates the access agreements as part of the system security authorization or when a contract is renewed or extended, but minimally within every three hundred sixty-five (365) days, whichever occurs first; and
c. Ensures that individuals requiring access to organizational information and information systems:
1. Acknowledge (paper or electronic) appropriate access agreements prior to being granted access; and
2. Re-acknowledge access agreements to maintain access to organizational information systems when access agreements have been updated.

Guidance
Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

PS-6 Compliance Description:

PS-7 – Third-Party Personnel Security

CMS ARS Mod 2.0 - Control:
The organization:
a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
c. Documents personnel security requirements;
d. Requires third-party providers to notify Contracting Officers or Contracting Officer Representatives (via the roster of contractor personnel) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within fifteen (15) calendar days; and
e. Monitors provider compliance.

Implementation Standard(s)
1. Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support information security policies and standards.

Guidance
Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated.

PS-7 Compliance Description:

PS-8 – Personnel Sanctions

CMS ARS Mod 2.0 - Control:
The organization:
a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notifies defined personnel or roles (defined in the applicable security plan) within defined time period (defined in the applicable security plan) when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Guidance
Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

PS-8 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Contingency Planning (CP) Controls

CP-1 – Contingency Planning Policy and Procedures

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
b. Reviews and updates (as necessary) the current:
1. Contingency planning policy within every three hundred sixty-five (365) days; and
2. Contingency planning procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

CP-1 Compliance Description:

CP-2 Contingency Plan

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops a contingency plan for the information system in accordance with NIST SP 800-34 that:
1. Identifies essential CMS missions and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
4. Addresses maintaining essential CMS missions and business functions despite an information system disruption, compromise, or failure;
5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
6. Is reviewed and approved by designated officials within the organization;
b. Distributes copies of the contingency plan to the Information System Security Officer, Business Owner, Contingency Plan Coordinator, and other stakeholders identified within the contingency plan;
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for the information system within every three hundred sixty-five (365) days;
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes to key contingency personnel and organizational elements identified above; and
g. Protects the contingency plan from unauthorized disclosure and modification.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to distribute the contingency plan to. The contingency list includes designated FedRAMP personnel.
2. **(For CSP only)** For service providers, the organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to communicate any contingency plan changes to. The contingency list includes designated FedRAMP personnel.

Guidance
Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident.

CP-2 Compliance Description:

CP-2(1) - Coordinate with Related Plans – Enhancement

CMS ARS Mod 2.0 - Control:
The organization coordinates contingency plan development with organizational elements responsible for related plans.

Guidance
Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

CP-2(1) Compliance Description:

CP-2(2) - Capacity Planning – Enhancement

CMS ARS Mod 2.0 - Control:
The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Guidance
Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning.

CP-2(2) Compliance Description:

CP-2(3) - Resume Essential Missions/Business Functions – Enhancement

CMS ARS Mod 2.0 - Control:
The organization plans for the resumption of essential missions and business functions within the approved Maximum Tolerable Downtime (MTD) for the business functions.

Guidance
Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure.

CP-2(3) Compliance Description:

CP-2(8) - Identify Critical Assets – Enhancement

CMS ARS Mod 2.0 - Control:
The organization identifies critical information system assets supporting essential missions and business functions.

Guidance
Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets.

CP-2(8) Compliance Description:

CP-3 – Contingency Training

CMS ARS Mod 2.0 - Control:
The organization provides contingency training to operational and support personnel (including managers and information system users) consistent with assigned roles and responsibilities:
a. Within ninety (90) days of assuming a contingency role or responsibility;
b. When required by information system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

Guidance
Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan. Managers, responsible for contingency operations, and technical personnel should meet, at a minimum, once a year for review of contingency policies and procedures. Each review session should be documented and confirmed that appropriate training has been completed.

CP-3 Compliance Description:

CP-4 – Contingency Plan Testing

CMS ARS Mod 2.0 - Control:
The organization:
a. Tests the contingency plan for the information system within every three hundred sixty-five (365) days using NIST or CMS defined tests and exercises, such as the tabletop test in accordance with the current CMS contingency plan procedure to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization tests and/or exercises the contingency plan for the information system at least annually using functional exercises to determine the plan's effectiveness and the organization's readiness to execute the plan.

Guidance
Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

CP-4 Compliance Description:

CP-4(1) - Coordinate with Related Plans – Enhancement

CMS ARS Mod 2.0 - Control:
The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Guidance
Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements.

CP-4(1) Compliance Description:

CP-6 – Alternate Storage Site

CMS ARS Mod 2.0 - Control:
The organization:
a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Guidance
Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.

CP- 6 Compliance Description:

CP-6(1) - Separation from Primary Site – Enhancement

CMS ARS Mod 2.0 - Control:
The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Guidance
Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant.

CP-6(1) Compliance Description:

CP-6(3) - Accessibility – Enhancement

CMS ARS Mod 2.0 - Control:
The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Guidance
Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

CP-6(3) Compliance Description:

CP-7 – Alternate Processing Site

CMS ARS Mod 2.0 - Control:
The organization:
a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within the time period specified in Implementation Standard 1 when the primary processing capabilities are unavailable; and
b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

Implementation Standard(s)
1. Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of system Recovery Time Objectives (RTOs) and business function Maximum Tolerable Downtimes (MTDs).
2. **(For CSP only)** For service providers, the organization defines a resumption time period consistent with the recovery time objectives and business impact analysis. The time period is approved and accepted by the Joint Authorization Board (JAB).

Guidance
Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.
Equipment and supplies required to resume operations within the CMS-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with CMS recovery time objectives.

CP-7 Compliance Description:

CP-7(1) - Separation from Primary Site – Enhancement

CMS ARS Mod 2.0 - Control:
The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

Guidance
Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant.

CP-7(1) Compliance Description:

CP-7(2) - Accessibility – Enhancement

CMS ARS Mod 2.0 - Control:
The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Guidance
Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk.

CP-7(2) Compliance Description:

CP-7(3) - Priority of Service – Enhancement

CMS ARS Mod 2.0 - Control:
The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organizational availability requirements (including recovery time objectives).

Guidance
Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availabilityrequirements and the availability of information resources at the alternate processing site.

CP-7(3) Compliance Description:

CP-8 – Telecommunications Services

CMS ARS Mod 2.0 - Control:
The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential CMS missions and business functions within the resumption time period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Implementation Standard(s)
1. Ensure alternate telecommunications Service Level Agreements (SLAs) are in place to permit resumption of system Recovery Time Objectives (RTOs) and business function Maximum Tolerable Downtimes (MTDs).
2. **(For CSP only)** For service providers, the organization defines a resumption time period consistent with the recovery time objectives and business impact analysis. The time period is approved and accepted by the Joint Authorization Board (JAB).

Guidance
This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

CP-8 Compliance Description:

CP-8(1) - Priority of Service Provisions – Enhancement

CMS ARS Mod 2.0 - Control:
The organization:
(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Guidance
Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-ofservice provisions.

CP-8(1) Compliance Description:

CP-8(2) - Single Points of Failure – Enhancement

CMS ARS Mod 2.0 - Control:
The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Guidance
None

CP-8(2) Compliance Description:

CP-9 – Information System Backup (Moderate) P1

CMS ARS Mod 2.0 - Control:
The organization:
a. Conducts backups of user-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1;
b. Conducts backups of system-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1;
c. Conducts backups of information system documentation including security-related documentation and other forms of data, including paper records within the defined frequency (defined in the applicable security plan) consistent with recovery time and recovery point objectives; and
d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Implementation Standard(s)
1. Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Three (3) generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups must be logged with name, date, time and action.
2. **(For PII only)** Ensure that a current, retrievable, copy of PII is available before movement of servers.
3. **(For CSP only)** For service providers, these Standards replace the above Control and Standard. The organization shall determine what elements of the cloud environment require the Information System Backup control. The cloud environment elements requiring Information System Backup are approved and accepted by the Joint Authorization Board (JAB).
4. **(For CSP only)** For service providers, the organization determines how Information System Backup is going to be verified and appropriate periodicity of the check. The verification and periodicity of the Information System Backup are approved and accepted by the Joint Authorization Board (JAB).
5. **(For CSP only)** For service providers, the organization:
a. Conducts backups of user-level information contained in the information system daily incremental; weekly full;
b. Conducts backups of system-level information contained in the information system daily incremental; weekly full;
c. Conducts backups of information system documentation including security-related documentation daily incremental; weekly full.
6. **(For CSP only)** For service providers, the organization maintains at least three (3) backup copies of user-level information (at least one (1) of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the Joint Authorization Board (JAB).
7. **(For CSP only)** For service providers, the organization maintains at least three (3) backup copies of system-level information (at least one (1) of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the Joint Authorization Board (JAB).
8. **(For CSP only)** For service providers, the organization maintains at least three (3) backup copies of information system documentation including security information (at least one (1) of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the Joint Authorization Board (JAB).

Guidance
System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information.
The transfer rate of backup information to an alternate storage site (if so designated) is guided by the CMS recovery time objectives and recovery point objectives. Checkpoint capabilities are part of any backup operation that updates files and consumes large amounts of information system time.

CP-9 Compliance Description:

CP-9(1) - Testing for Reliability/Integrity – Enhancement

CMS ARS Mod 2.0 - Control:
The organization tests backup information following each backup to verify media reliability and information integrity.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The organization tests backup information at least annually.

Guidance
None

CP-9(1) Compliance Description:

CP-9(3) - Separate Storage for Critical Information – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

Guidance
(For CSP only) Critical information system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations.

CP-9(3) Compliance Description:

CP-10 – Information System Recovery and Reconstitution

CMS ARS Mod 2.0 - Control:
The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.

Implementation Standard(s)
1. Secure information system recovery and reconstitution includes, but not limited to:
(a) Reset all system parameters (either default or organization-established),
(b) Reinstall patches,
(c) Reestablish configuration settings,
(d) Reinstall application and system software, and
(e) Fully test the system.

Guidance
Recovery is executing information system contingency plan activities to restore CMS missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures.

CP-10 Compliance Description:

CP-10(2) - Transaction Recovery – Enhancement

CMS ARS Mod 2.0 - Control:
The information system implements transaction recovery for systems that are transaction-based.

Guidance
Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

CP-10(2) Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Maintenance (MA) Controls

MA-1 – System Maintenance Policy and Procedures

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
b. Reviews and updates (as necessary) the current:
1. System maintenance policy within every three hundred sixty-five (365) days; and
2. System maintenance procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

MA-1 Compliance Description:

MA-2 – Controlled Maintenance

CMS ARS Mod 2.0 - Control:
The organization:
a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
c. Requires that the applicable Business Owner (or an official designated in the applicable security plan) explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
f. Includes defined maintenance-related information (defined in the applicable security plan) in organizational maintenance records.

Implementation Standard(s)
1. **(For PII only)** In facilities where PII is stored or accessed, document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Guidance
This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems.

MA-2 Compliance Description:

MA-3 – Maintenance Tools

CMS ARS Mod 2.0 - Control:
The organization approves, controls, and monitors information system maintenance tools.

Guidance
This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch.

MA-3 Compliance Description:

MA-3(1) - Inspect Tools – Enhancement

CMS ARS Mod 2.0 - Control:
The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Guidance
If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

MA-3(1) Compliance Description:

MA-3(2) - Inspect Media – Enhancement

CMS ARS Mod 2.0 - Control:
The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

Guidance
If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

MA-3(2) Compliance Description:

MA-3(3) - Prevent Unauthorized Removal – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:
(a) Verifying that there is no organizational information contained on the equipment;
(b) Sanitizing or destroying the equipment;
(c) Retaining the equipment within the facility; or
(d) Obtaining an exemption, in writing, from the CMS CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no sensitive information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.

Guidance
(For CSP only) Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.

MA-3(3) Compliance Description:

MA-4 – Nonlocal Maintenance

CMS ARS Mod 2.0 - Control:
The organization monitors and controls nonlocal maintenance and diagnostic activities; and prohibits nonlocal system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If nonlocal maintenance and diagnostic actives are authorized, the organization:
a. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
b. Employs strong identification and authentication techniques in the establishment of nonlocal maintenance and diagnostic sessions;
c. Maintains records for nonlocal maintenance and diagnostic activities; and
d. Terminates all sessions and network connections when nonlocal maintenance is completed.

Implementation Standard(s)
1. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service.

Guidance
Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part by other controls.

MA-4 Compliance Description:

MA-4(1) - Auditing and Review – Enhancement

CMS ARS Mod 2.0 - Control:
The organization:
(a) Audits nonlocal maintenance and diagnostic sessions using available audit events; and
(b) Reviews the records of the maintenance and diagnostic sessions.

Guidance
None

MA-4(1) Compliance Description:

MA-4(2) - Document Nonlocal Maintenance – Enhancement

CMS ARS Mod 2.0 - Control:
The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

Guidance
None

MA-4(2) Compliance Description:

MA-4(3) - Comparable Security/Sanitization – Enhancement

CMS ARS Mod 2.0 - Control:
The organization:
(a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or
(b) Removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.

Guidance
Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced.

MA-4(3) Compliance Description:

MA-5 – Maintenance Personnel

CMS ARS Mod 2.0 - Control:
The organization:
a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Guidance
This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, system integrators, and consultants, may require privileged access to organizational information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

MA-5 Compliance Description:

MA-6 – Timely Maintenance

CMS ARS Mod 2.0 - Control:
The organization obtains maintenance support and/or spare parts for defined key information system components (defined in the applicable security plan) within the applicable Recovery Time Objective (RTO) specified in the contingency plan.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Control. The organization defines a list of security-critical information system components and/or key information technology components. The list of components is approved and accepted by the Joint Authorization Board (JAB).
2. **(For CSP only)** For service providers, the organization defines a time period to obtain maintenance and spare parts in accordance with the contingency plan for the information system and business impact analysis. The time period is approved and accepted by the Joint Authorization Board (JAB).

Guidance
Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place.

MA-6 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Media Protection (MP) Controls

MP-1 – Media Protection Policy and Procedures

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
b. Reviews and updates (as necessary) the current:
1. Media protection policy within every three hundred sixty-five (365) days; and
2. Media protection procedures within every three hundred sixty-five (365) days.

Implementation Standard(s)
1. **(For PII only)** Semi-annual inventories of magnetic tapes containing PII are conducted. The organization accounts for any missing tape containing PII by documenting the search efforts and notifying the tape initiator of the loss.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

MP-1 Compliance Description:

MP-2 – Media Access

CMS ARS Mod 2.0 - Control:
The organization restricts access to sensitive digital and non-digital media defined within NIST SP 800-88, Guidelines for Media Sanitization, to defined personnel or roles (defined in the applicable security plan) by disabling:
- CD/DVD writers and allowing access to defined personnel or roles; and
- USB ports and allowing access to defined personnel or roles.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Control. The organization defines types of digital and non-digital media. The media types are approved and accepted by the Joint Authorization Board (JAB).
2. **(For CSP only)** For service providers, the organization defines a list of individuals with authorized access to defined media types. The list of authorized individuals is approved and accepted by the JAB.
3. **(For CSP only)** For service providers, the organization defines the types of security measures to be used in protecting defined media types. The security measures are approved and accepted by the JAB.

Guidance
Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.

MP-2 Compliance Description:

MP-3 – Media Marking

CMS ARS Mod 2.0 - Control:
The organization:
a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempts specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking as long as the media remain within a secure environment.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization does not exempt any removable media types from marking.

Guidance
The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes with regard to internal data structures within information systems (see AC-16). Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

MP-3 Compliance Description:

MP-4 – Media Storage

CMS ARS Mod 2.0 - Control:
The organization:
a. Physically controls and securely stores digital and non-digital media defined within NIST SP 800-88, Guidelines for Media Sanitization, within controlled areas; and
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Implementation Standard(s)
1. **(For PII only)** Evaluate employing an approved method of cryptography (see SC-13) to protect PII at rest, consistent with NIST SP 800-66 guidance.
2. **(For PII only)** If PII is recorded on magnetic media with other data, it should be protected as if it were entirely personally identifiable information.
3. **(For CSP only)** For service providers, this Standard replaces the above Control. The organization physically controls and securely stores magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks within organization-defined controlled areas using for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secure storage in locked cabinets or safes.
4. **(For CSP only)** For service providers, the organization defines controlled areas within facilities where the information and information system reside.

Guidance
Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas or spaces for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

MP-4 Compliance Description:

MP-5 – Media Transport

CMS ARS Mod 2.0 - Control:
The organization:
a. Protects and controls digital and non-digital media defined within NIST SP 800-88, Guidelines for Media Sanitization, containing sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging and (i) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (ii) if shipped, trackable with receipt by commercial carrier;
b. Maintains accountability for information system media during transport outside of controlled areas;
c. Documents activities associated with the transport of information system media; and
d. Restricts the activities associated with the transport of information system media to authorized personnel.

Implementation Standard(s)
1. **(For PII only)** Protect and control PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. PII must be in locked cabinets or sealed packing cartons while in transit.
2. **(For FTI only)** Organizations are not allowed to make further disclosures of FTI to their agents or to a contractor unless authorized by statute. (See IRS Pub. 1075, sect. 11.1 and 5.9)
3. **(For CSP only)** For service providers, the organization protects and controls magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks during transport outside of controlled areas using for digital media, encryption using a FIPS 140-2 validated encryption module.
4. **(For CSP only)** For service providers, the organization defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB.

Guidance Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.
Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records.

MP-5 Compliance Description:

MP-5(4) - Cryptographic Protection – Enhancement

CMS ARS Mod 2.0 - Control:
The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Guidance
This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers).

MP-5(4) Compliance Description:

MP-6 – Media Sanitization

CMS ARS Mod 2.0 - Control:
The organization:
a. Sanitizes both digital and non-digital information system media prior to disposal, release out of organizational control, or release for reuse using defined sanitization techniques and procedures (defined in the applicable security plan) in accordance with applicable federal and organizational standards and policies; and
b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Implementation Standard(s)
1. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.
2. **(For FTI only)** FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the Internal Revenue Code. Generally, destruction should be witnessed by an agency employee.
3. **(For PII only)** Authorized employees of the receiving entity must be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies:
- date received
- reel/cartridge control number contents
- number of records, if available
- movement, and
- if disposed of, the date and method of disposition.
4. Surplus equipment is stored securely while not in use, and disposed of or sanitized in accordance with NIST SP 800-88 when no longer required.

Guidance
This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information.

MP-6 Compliance Description:

MP-6(1) - Review/Approve/Track/Document/Verify – Enhancement

CMS ARS Mod 2.0 - Control:
MP-6(1) - Review/Approve/Track/Document/Verify – Enhancement (Moderate) P1
Control
The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Guidance
Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal.

MP-6(1) Compliance Description:

MP-6(2) - Equipment Testing – Enhancement

CMS ARS Mod 2.0 - Control:
The organization tests sanitization equipment and procedures within every three hundred sixty-five (365) days to verify that the intended sanitization is being achieved.

Guidance
Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other federal agencies or external service providers).

MP-6(2) Compliance Description:

MP-7 – Media Use

CMS ARS Mod 2.0 - Control:
The organization prohibits the use of personally owned media on organizational information systems or system components using defined security safeguards (defined in the applicable security plan).

Guidance
Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices.

MP-7 Compliance Description:

MP-7(1) - Prohibit Use Without Owner – Enhancement

CMS ARS Mod 2.0 - Control:
MP-7(1) - Prohibit Use Without Owner – Enhancement (Moderate) P1
Control
The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Guidance
Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion).

MP-7(1) Compliance Description:

MP-CMS-1 – Media Related Records

CMS ARS Mod 2.0 - Control:
Inventory and disposition records for information system media shall be maintained to ensure control and accountability of sensitive information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach.

Implementation Standard(s)
1. The media records must, at a minimum, contain:
(a) The name of media recipient;
(b) Signature of media recipient;
(c) Date/time media received;
(d) Media control number and contents;
(e) Movement or routing information; and
(f) If disposed of, the date, time, and method of destruction.

Guidance
Employing a hash function (a reproducible method of turning inventory data into a relatively small number may serve as a digital "fingerprint" of the data) for electronic inventory records maintenance so the inventory information can be validated as not being tampered with prior to reconstructive events for an investigation of a possible breach.

MP-CMS-1 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Physical and Environmental Protection (PE) Controls

PE-1 – Physical and Environmental Protection Policy and Procedures

CMS ARS Mod 2.0 - Control:
PE-1 – Physical and Environmental Protection Policy and Procedures (Moderate) Assurance - P1
Control
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
b. Reviews and updates (as necessary) the current:
1. Physical and environmental protection policy within every three hundred sixty-five (365) days; and
2. Physical and environmental protection procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

PE-1 Compliance Description:

PE-2 – Physical Access Authorizations

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
b. Issues authorization credentials for facility access;
c. Reviews the access list detailing authorized facility access by individuals in accordance with the frequency specified in Implementation Standard 1; and
d. Removes individuals from the facility access list when access is no longer required.

Implementation Standard(s)
1. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every one hundred eighty (180) days.
2. **(For PII only)** Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly.
3. **(For CSP only)** For service providers, the organization reviews and approves the access list and authorization credentials at least annually, removing from the access list personnel no longer requiring access.

Guidance
This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible.

PE-2 Compliance Description:

PE-3 – Physical Access Control

CMS ARS Mod 2.0 - Control:
The organization:
a. Enforces physical access authorizations at defined entry/exit points to the facility (defined in the applicable security plan) where the information system resides] by;
1. Verifying individual access authorizations before granting access to the facility; and
2. Controlling ingress/egress to the facility using guards and/or defined physical access control systems/devices (defined in the applicable security plan);
b. Maintains physical access audit logs for defined entry/exit points (defined in the applicable security plan);
c. Provides defined security safeguards (defined in the applicable security plan) to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan);
e. Secures keys, combinations, and other physical access devices;
f. Inventories defined physical access devices (defined in the applicable security plan) with the frequency specified in Implementation Standard 5; and
g. Changes combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) within every three hundred sixty-five (365) days, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Implementation Standard(s)
1. Control data center/facility access by use of door and window locks, and security personnel or physical authentication devices, such as biometrics and/or smart card/PIN combination.
2. Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded.
3. Restrict access to grounds/facilities to authorized persons only.
4. **(For PII only)** Require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protected information must be containerized in areas where other than authorized employees may have access afterhours.
5. Conducts inventories of physical access devices within every ninety (90) days.
6. **(For CSP only)** For service providers, the organization inventories physical access devices at least annually.

Guidance
This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices.

PE- 3 Compliance Description:

PE-4 – Access Control for Transmission Medium

CMS ARS Mod 2.0 - Control:
The organization controls physical access to telephone closets and information system distribution and transmission lines within organizational facilities using defined security safeguards (defined in the applicable security plan).

Implementation Standard(s)
1. Disable any physical ports (e.g., wiring closets, patch panels, etc.) not in use.

Guidance
Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

PE-4 Compliance Description:

PE-5 – Access Control for Output Devices

CMS ARS Mod 2.0 - Control:
The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Guidance
Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

PE-5 Compliance Description:

PE-6 – Monitoring Physical Access

CMS ARS Mod 2.0 - Control:
The organization:
a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Reviews physical access logs weekly and upon occurrence of security incidents involving physical security; and
c. Coordinates results of reviews and investigations with the organization's incident response capability.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization reviews physical access logs at least semi-annually.

Guidance
Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses.

PE-6 Compliance Description:

PE-6(1) - Intrusion Alarms/Surveillance Equipment – Enhancement

CMS ARS Mod 2.0 - Control:
The organization monitors physical intrusion alarms and surveillance equipment.

Guidance
None

PE-6(1) Compliance Description:

PE-8 – Visitor Access Records

CMS ARS Mod 2.0 - Control:
The organization:
a. Maintains visitor access records to the facility where the information system resides for two (2) years; and
b. Reviews visitor access records at least monthly.

Guidance
Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas. See NARA Schedule 18 for additional detail on this requirement.

PE-8 Compliance Description:

PE-9 – Power Equipment and Cabling

CMS ARS Mod 2.0 - Control:
The organization protects power equipment and power cabling for the information system from damage and destruction.

Implementation Standard(s)
1. Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

Guidance
Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.

PE-9 Compliance Description:

PE-10 – Emergency Shutoff

CMS ARS Mod 2.0 - Control:
The organization:
a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
b. Places emergency shutoff switches or devices in a location that does not require personnel to approach the equipment to facilitate safe and easy access for personnel;
c. Protects emergency power shutoff capability from unauthorized activation; and
d. Implements and maintains a master power switch or emergency cut-off switch, prominently marked and protected by a cover, for data centers, servers, and mainframe rooms.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization defines emergency shutoff switch locations. The locations are approved and accepted by the JAB.

Guidance
This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

PE-10 Compliance Description:

PE-11 – Emergency Power

CMS ARS Mod 2.0 - Control:
The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Guidance
None

PE-11 Compliance Description:

PE-12 – Emergency Lighting

CMS ARS Mod 2.0 - Control:
The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility.

Guidance
This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

PE-12 Compliance Description:

PE-13 – Fire Protection

CMS ARS Mod 2.0 - Control:
The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Guidance
This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

PE-13 Compliance Description:

PE-13(1) - Detection Devices/Systems – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs fire detection devices/systems for the information system that activate automatically and notify defined personnel or roles (defined in the applicable security plan) and defined emergency responders (defined in the applicable security plan) in the event of a fire.

Guidance
Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

PE-13(1) Compliance Description:

PE-13(2) - Suppression Devices/Systems – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to defined personnel (or roles) and defined emergency responders (defined in the applicable security plan).

Guidance
Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

PE-13(2) Compliance Description:

PE-13(3) - Automatic Fire Suppression – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

Guidance
None

PE-13(3) Compliance Description:

PE-14 – Temperature and Humidity Controls

CMS ARS Mod 2.0 - Control:
The organization:
a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels; and
b. Monitors temperature and humidity levels within the defined frequency (defined in the applicable security plan).

Implementation Standard(s)
1. Evaluate the level of alert and follow prescribed guidelines for that alert level.
2. Alert component management of possible loss of service and/or media.
3. Report damage and provide remedial action. Implement contingency plan, if necessary.
4. **(For CSP only)** For service providers, this Standard replaces the above Control. The organization:
a. Maintains temperature and humidity levels within the facility where the information system resides at levels consistent with American Society of Heating, Refrigerating and Airconditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments; and
b. Monitors temperature and humidity levels continuously.
5. **(For CSP only)** For service providers, the organization measures temperature at server inlets and humidity levels by dew point.

Guidance
This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.

PE-14 Compliance Description:

PE-15 – Water Damage Protection

CMS ARS Mod 2.0 - Control:
The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Guidance
This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.

PE-15 Compliance Description:

PE-16 – Delivery and Removal

CMS ARS Mod 2.0 - Control:
The organization authorizes, monitors, and controls the flow of information system-related components entering and exiting the facility and maintains records of those items.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Control. The organization authorizes, monitors, and controls the flow of all information system components entering and exiting the facility and maintains records of those items.

Guidance
Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

PE-16 Compliance Description:

PE-17 – Alternate Work Site

CMS ARS Mod 2.0 - Control:
The organization:
a. Employs appropriate security controls at alternate work sites to include, but not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems at alternate work sites;
b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization defines management, operational, and technical information system security controls for alternate work sites. The security controls are approved and accepted by the JAB.

Guidance
Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations and the federal telework initiative.

PE-17 Compliance Description:

PE-18 – Location of Information System Components

CMS ARS Mod 2.0 - Control:
The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards, and to minimize the opportunity for unauthorized access.

Guidance
Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones).

PE-18 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

System and Services Acquisition (SA) Controls

SA-1 – System and Services Acquisition Policy and Procedures

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
b. Reviews and updates (as necessary) the current:
1. System and services acquisition policy within every three hundred sixty-five (365) days; and
2. System and services acquisition procedures within every three hundred sixty-five (365) days.

Implementation Standard(s)
1. **(For FTI only)** Develop, disseminates, and periodically reviews/updates a formal, documented, system and services acquisition policy that includes IRS documents received and identified by:
(a) Taxpayer name
(b) Tax year(s)
(c) Type of information (e.g., revenue agent reports, Form 1040, work papers)
(d) The reason for the request
(e) Date requested
(f) Date received
(g) Exact location of the FTI
(h) Who has had access to the data and
(i) If disposed of, the date and method of disposition.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

SA-1 Compliance Description:

SA-2 – Allocation of Resources

CMS ARS Mod 2.0 - Control:
The organization:
a. Determines information security requirements for the information system or information system service in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process;
c. Includes information security requirements in mission/business case planning, and
d. Establishes a discrete line item in CMS' programming and budgeting documentation for the implementation and management of information systems security.

Guidance
Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service.

SA-2 Compliance Description:

SA-3 – System Development Life Cycle

CMS ARS Mod 2.0 - Control:
The organization:
a. Manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS eXpedited Life Cycle (XLC) that incorporates information security control considerations;
b. Defines and documents information security roles and responsibilities throughout the system development life cycle;
c. Identifies individuals having information system security roles and responsibilities; and
d. Integrates the organizational information security risk management process into system development life cycle activities.

Guidance
A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life
cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies.

SA-3 Compliance Description:

SA-4 – Acquisition Process

CMS ARS Mod 2.0 - Control:
The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:
a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Requirements for protecting security-related documentation;
f. Description of the information system development environment and environment in which the system is intended to operate; and
g. Acceptance criteria.

Implementation Standard(s)
1. Each contract and Statement of Work (SOW) that requires development or access to CMS information must include language requiring adherence to CMS security and privacy policies and standards, define security and privacy roles and responsibilities, and receive approval from CMS officials.

Guidance
Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle.
Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA.
(For CSP only) The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred. See http://www.niap-ccevs.org/vpl or http://www.commoncriteriaportal.org/products.html.

SA-4 Compliance Description:

SA-4(1) - Functional Properties of Security Controls – Enhancement

CMS ARS Mod 2.0 - Control:
The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Guidance
Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

SA-4(1) Compliance Description:

SA-4(2) - Design/Implementation Information for Security Controls – Enhancement

CMS ARS Mod 2.0 - Control:
The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation.

Guidance
Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of multiple subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information system.

SA-4(2) Compliance Description:

SA-4(7) - NIAP-Approved Protection Profiles – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the organization:
(a) Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and
(b) Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.

Guidance
None

SA-4(7) Compliance Description:

SA-4(9) - Functions/Ports/Protocols/Services In Use – Enhancement

CMS ARS Mod 2.0 - Control:
The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

Guidance
The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented. SA-9 describes requirements for external information system services with organizations identifying which functions, ports, protocols, and services are provided from external sources.

SA-4(9) Compliance Description:

SA-4(10) - Use of Approved PIV Products – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Guidance
None

SA-4(10) Compliance Description:

SA-5 – Information System Documentation

CMS ARS Mod 2.0 - Control:
The organization:
a. Obtains administrator documentation for the information system, system component, or information system service that describes:
1. Secure configuration, installation, and operation of the system, component, or service;
2. Effective use and maintenance of security functions/mechanisms; and
3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
b. Obtains user documentation for the information system, system component, or information system service that describes:
1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
3. User responsibilities in maintaining the security of the system, component, or service;
c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent, and evaluate whether such documentation is essential for the effective implementation or operation of security controls;
d. Protects documentation as required, in accordance with the risk management strategy; and
e. Distributes documentation to defined personnel or roles (defined in the applicable security plan).

Implementation Standard(s)
1. Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.
2. Maintain an updated list of related system operations and security documentation.
3. Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation.

Guidance
This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation.

SA-5 Compliance Description:

SA-8 – Security Engineering Principles

CMS ARS Mod 2.0 - Control:
The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Guidance
Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

SA-8 Compliance Description:

SA-9 – External Information System Services

CMS ARS Mod 2.0 - Control:
The organization:
a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Employs defined processes, methods, and techniques (defined in the applicable security plan) to monitor security control compliance by external service providers on an ongoing basis.

Implementation Standard(s)
1. **(For PHI only)** A covered entity or business associate under HIPAA or HITECH may create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations. (See HIPAA 164.308(b), 164.314(a), and 164.530.)

Guidance
External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

SA-9 Compliance Description:

SA-9(1) - Risk Assessments/Organizational Approvals – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the organization:
(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and
(b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by Joint Authorization Board (JAB).

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. Future, planned outsourced services are approved and accepted by the JAB.

Guidance
(For CSP only) Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services.

SA-9(1) Compliance Description:

SA-9(2) - Identification of Functions/Ports/Protocols/Services – Enhancement

CMS ARS Mod 2.0 - Control:
The organization requires providers of defined external information system services (defined in the applicable security plan) to identify the functions, ports, protocols, and other services required for the use of such services.

Guidance
Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols.

SA-9(2) Compliance Description:

SA-10 – Developer Configuration Management

CMS ARS Mod 2.0 - Control:
The organization requires the developer of the information system, system component, or information system service to:
a. Perform configuration management during system, component, or service development, implementation, and operation;
b. Document, manage, and control the integrity of changes to configuration items under configuration management;
c. Implement only organization-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to defined personnel or roles (defined in the applicable security plan).

Guidance
This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle.

SA-10 Compliance Description:

SA-11 – Developer Security Testing and Evaluation

CMS ARS Mod 2.0 - Control:
The organization requires the developer of the information system, system component, or information system service to:
a. Create and implement a security assessment plan in accordance with, but not limited to, current CMS procedures;
b. Perform unit; integration; system; regression testing/evaluation in accordance with the CMS eXpedited Life Cycle (XLC);
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during security testing/evaluation.

Implementation Standard(s)
1. If the security control assessment results are used in support of the security authorization process for the information system, ensure that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results.
2. Use hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.
3. All systems supporting development and pre-production testing are connected to an isolated network separated from production systems. Network traffic into and out of the development and pre-production testing environment is only permitted to facilitate system testing, and is restricted by source and destination access control lists (ACLs) as well as ports and protocols.

Guidance
Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.

SA-11 Compliance Description:

SA-11(1) - Static Code Analysis – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization submits a code analysis report as part of the authorization package and update the report in any reauthorization actions.
2. **(For CSP only)** For service providers, the organization documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

Guidance
(For CSP only) Static code analysis provides a technology and methodology for security reviews. Such analysis can be used to identify security vulnerabilities and enforce security coding practices. Static code analysis is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were fixed. An excessively high density of ignored findings (commonly referred to as ignored or false positives) indicates a potential problem with the analysis process or tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

SA-11(1) Compliance Description:

SA-12 – Supply Chain Protection

CMS ARS Mod 2.0 - Control:
(For CSP only) The organization protects against supply chain threats to the information system, system component, or information system service by employing best practices and methodologies; and wherever possible, selecting components that have been previously reviewed by other government entities (e.g., National Information Assurance Partnership [NIAP]) as part of a comprehensive, defense-in-breadth information security strategy.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Control. The organization protects against supply chain threats by employing organization-defined list of measures to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy.
2. **(For CSP only)** For service providers, the organization defines a list of types of denial of service attacks (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list. The list of denial of service attack types is approved and accepted by JAB.

Guidance
(For CSP only) Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control
enhancement also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.

SA-12 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

System and Communications Protection (SC) Controls

SC-1 – System and Communications Protection Policy and Procedures

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
b. Reviews and updates (as necessary) the current:
1. System and communications protection policy within every three hundred sixty-five (365) days; and
2. System and communications protection procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

SC-1 Compliance Description:

SC-2 – Application Partitioning

CMS ARS Mod 2.0 - Control:
The information system separates user functionality (including user interface services) from information system management functionality.

Guidance
Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

SC-2 Compliance Description:

SC-4 – Information in Shared Resources

CMS ARS Mod 2.0 - Control:
The information system prevents unauthorized and unintended information transfer via shared system resources.

Implementation Standard(s)
1. Ensure that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. Ensure that system resources shared between two (2) or more users are released back to the information system, and are protected from accidental or purposeful disclosure.
2. **(For FTI only)** When authorized to make further disclosures is present (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting FTI from one computer to another need only identify the bulk records transmitted. This identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.

Guidance
This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles.

SC-4 Compliance Description:

SC-5 – Denial of Service Protection

CMS ARS Mod 2.0 - Control:
The information system protects against or limits the effects of the types of denial of service attacks defined in NIST SP 800-61, Computer Security Incident Handling Guide, and the following websites by employing defined security safeguards (defined in the applicable security plan):
- SANS Organization: www.sans.org/dosstep;
- SANS Organization's Roadmap to Defeating DDoS: www.sans.org/dosstep/roadmap.php; and
- NIST National Vulnerability Database: http://nvd.nist.gov/home.cfm.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization defines a list of types of denial of service attacks (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list. The list of denial of service attack types is approved and accepted by JAB.

Guidance
A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.

SC-5 Compliance Description:

SC-6 – Resource Availability

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the information system protects the availability of resources by allocating (FedRAMP-defined) resources by priority and/or quota (FedRAMP-defined), and other FedRAMP-defined safeguards for this control.

Guidance
(For CSP only) Priority protection helps prevent lower-priority processes from delaying or interfering with the information system servicing any higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to information system components for which there are only single users/roles.

SC-6 Compliance Description:

SC-7 – Boundary Protection

CMS ARS Mod 2.0 - Control:
The information system:
a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
b. Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and
c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Implementation Standard(s)
1. Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.
2. Utilize stateful inspection/application firewall hardware and software.
3. Utilize firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

Guidance
Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.

SC-7 Compliance Description:

SC-7(3) - Access Points – Enhancement

CMS ARS Mod 2.0 - Control:
The organization limits the number of external network connections to the information system.

Guidance
Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections.

SC-7(3) Compliance Description:

SC-7(4) - External Telecommunications Services – Enhancement

CMS ARS Mod 2.0 - Control:
The organization:
(a) Implements a managed interface for each external telecommunication service;
(b) Establishes a traffic flow policy for each managed interface;
(c) Protects the confidentiality and integrity of the information being transmitted across each interface;
(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
(e) Reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days or implementation of major new system, and removes exceptions that are no longer supported by an explicit mission/business need.

Guidance
None

SC-7(4) Compliance Description:

SC-7(5) - Deny by Default/Allow by Exception – Enhancement

CMS ARS Mod 2.0 - Control:
The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

Guidance
This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

SC-7(5) Compliance Description:

SC-7(7) - Prevent Split Tunneling for Remote Devices – Enhancement

CMS ARS Mod 2.0 - Control:
The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

Guidance
This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. The use of VPNs for remote connections, when adequately provisioned with appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.

SC-7(7) Compliance Description:

SC-7(8) - Route Traffic to Authenticated Proxy Servers – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) The information system routes all user-initiated internal communications traffic to untrusted external networks through authenticated proxy servers at managed interfaces.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices.
2. **(For CSP only)** For service providers, the organization defines the internal communications traffic to be routed by the information system through authenticated proxy servers and the external networks that are the prospective destination of such traffic routing. The internal communications traffic and external networks are approved and accepted by JAB.

Guidance
(For CSP only) External networks are networks outside of organizational control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites.

SC-7(8) Compliance Description:

SC-7(12) - Host-Based Protection – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the organization implements FedRAMP defined host-based boundary protection mechanisms at FedRAMP defined information system components.

Guidance
(For CSP only) Host-based boundary protection mechanisms include, for example, host-based firewalls. Information system components employing host-based boundary protection mechanisms include, for example, servers, workstations, and mobile devices.

SC-7(12) Compliance Description:

SC-7(13) - Isolation of Security Tools/Mechanisms/Support Components – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the organization isolates organization-defined key information security tools, mechanisms, and support components from other internal information system components by implementing physically separate subnets with managed interfaces to other portions of the system.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization defines key information security tools, mechanisms, and support components associated with system and security administration; and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

Guidance
(For CSP only) Physically separate subnetworks with managed interfaces are useful, for example, in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques of organizations.

SC-7(13) Compliance Description:

SC-7(18) - Fail Secure – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the information system fails securely in the event of an operational failure of a boundary protection device.

Guidance
(For CSP only) Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones), information systems do not enter into unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases.

SC-7(18) Compliance Description:

SC-8 – Transmission Confidentiality and Integrity

CMS ARS Mod 2.0 - Control:
The information system protects the integrity of transmitted information.

Implementation Standard(s)
1. Employ appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13).

Guidance
This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing physical distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk.

SC-8 Compliance Description:

SC-8(1) - Cryptographic or Alternate Physical Protection – Enhancement

CMS ARS Mod 2.0 - Control:
The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by defined alternative physical safeguards (defined in the applicable security plan).

Guidance
Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems.

SC-8(1) Compliance Description:

SC-8(2) - Pre/Post Transmission Handling – Enhancement

CMS ARS Mod 2.0 - Control:
The information system maintains the confidentiality and integrity of information during preparation for transmission and during reception.

Guidance
Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception including, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

SC-8(2) Compliance Description:

SC-10 – Network Disconnect

CMS ARS Mod 2.0 - Control:
The information system terminates the network connection associated with a communications session at the end of the session, or:
a. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and
b. Forcibly disconnects inactive Virtual Private Network (VPN) connections after thirty (30) minutes or less of inactivity.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Control. The information system terminates the network connection associated with a communications session at the end of the session, or after thirty (30) minutes for all RAS-based sessions and thirty (30) to sixty (60) minutes for non-interactive users, of inactivity.

Guidance
This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses.
A session is an encounter between an end-user interface device (e.g., computer, terminal, process) and an application, including a network logon--the AC-11 session lock applies. A connection-based session is one that requires a connection to be established between hosts prior to an exchange of data.
(For CSP only) Long running batch jobs and other operations are not subject to this time limit.

SC-10 Compliance Description:

SC-11 – Trusted Path

SC-11 – Trusted Path (Moderate) Assurance - P0
(For CSP only) For service providers, the information system establishes a trusted communications path between the user and the FedRAMP security functions of the system, to include at a minimum, information system authentication and re-authentication.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization defines the security functions that require a trusted path, including but not limited to system authentication, reauthentication, and provisioning or de-provisioning of services (i.e. allocating additional bandwidth to a cloud user). The list of security functions requiring a trusted path is approved and accepted by JAB.

Guidance
(For CSP only) Trusted paths are mechanisms by which users (through input devices) can communicate directly with security functions of information systems with the requisite assurance to support information security policies. The mechanisms can be activated only by users or the security functions of organizational information systems. User responses via trusted paths are protected from modifications by or disclosure to untrusted applications. Organizations employ trusted paths for high-assurance connections between security functions of information systems and users (e.g., during system logons). Enforcement of trusted communications paths is typically provided via an implementation that meets the reference monitor concept.

SC-11 Compliance Description:

SC-12 – Cryptographic Key Establishment and Management

CMS ARS Mod 2.0 - Control:
When cryptography is required and used within the information system, the organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with defined requirements (defined in, or referenced by, the applicable security plan) for key generation, distribution, storage, access, and destruction.

Guidance
Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems.

SC-12 Compliance Description:

SC-12(2) - Symmetric Keys – Enhancement

CMS ARS Mod 2.0 - Control:
(For CSP only) For service providers, the organization produces, controls, and distributes symmetric cryptographic keys using NIST-approved key management technology and processes.

Guidance
None

SC-12(2) Compliance Description:

SC-13 – Cryptographic Protection

CMS ARS Mod 2.0 - Control:
When cryptographic mechanisms are used, the information system implements encryption products that have been validated under the Cryptographic Module Validation Program (see http://csrc.nist.gov/cryptval/) to confirm compliance with FIPS 140-2, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Guidance
Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPSvalidated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography).

SC-13 Compliance Description:

SC-15 – Collaborative Computing Devices

CMS ARS Mod 2.0 - Control:
The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If collaborative computer is authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used.
The information system:
a. Prohibits remote activation of collaborative computing devices; and
b. Provides an explicit indication of use to users physically present at the devices.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the information system prohibits remote activation of collaborative computing devices with no exceptions.
2. **(For CSP only)** For service providers, the information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

Guidance
Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

SC-15 Compliance Description:

SC-15(1) - Physical Disconnect – Enhancement

CMS ARS Mod 2.0 - Control:
If collaborative computing is authorized, the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

Guidance
Failing to physically disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session helps to ensure that participants actually carry out the disconnect activity without having to go through complex and tedious procedures.

SC-15(1) Compliance Description:

SC-17 – Public Key Infrastructure Certificates

CMS ARS Mod 2.0 - Control:
The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates from an approved service provider.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization defines the public key infrastructure certificate policy. The certificate policy is approved and accepted by the JAB.

Guidance
For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services.

SC-17 Compliance Description:

SC-18 – Mobile Code

CMS ARS Mod 2.0 - Control:
The organization:
a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

Guidance
Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems.

SC-18 Compliance Description:

SC-19 – Voice Over Internet Protocol

CMS ARS Mod 2.0 - Control:
The organization prohibits the use of Voice over Internet Protocol (VoIP) technologies, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If VoIP is authorized, the organization:
a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously;
b. Authorizes, monitors, and controls the use of VoIP within the information system; and
c. Ensures VoIP equipment used to transmit or discuss sensitive information is protected with FIPS 140-2 encryption standards.

Guidance
None

SC-19 Compliance Description:

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

CMS ARS Mod 2.0 - Control:
The information system:
a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Implementation Standard(s)
1. Recursive lookups are disabled on all publicly accessible domain name system (DNS) servers.

Guidance
This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data.

SC-20 Compliance Description:

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

CMS ARS Mod 2.0 - Control:
The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.

Guidance
Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.

SC-21 Compliance Description:

SC-22 – Architecture and Provisioning for Name/Address Resolution Service

CMS ARS Mod 2.0 - Control:
The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Guidance
Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists).

SC-22 Compliance Description:

SC-23 – Session Authenticity

CMS ARS Mod 2.0 - Control:
The information system protects the authenticity of communications sessions.

Guidance
This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.

SC-23 Compliance Description:

SC-28 – Protection of Information at Rest

CMS ARS Mod 2.0 - Control:
The information system protects the confidentiality and integrity of information at rest.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization supports the capability to use cryptographic mechanisms to protect information at rest.

Guidance
This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest.

SC-28 Compliance Description:

SC-30 – Concealment and Misdirection

CMS ARS Mod 2.0 - Control:
SC-30 – Concealment and Misdirection (Moderate) Assurance - P0
Control
(For CSP only) For service providers, the organization employs FedRAMP-defined concealment and misdirection techniques] for information systems, at FedRAMP-defined time periods, to confuse and mislead adversaries.

Guidance
(For CSP only) Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber attacks. For example, virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Increased use of concealment/misdirection techniques including, for example, randomness, uncertainty, and virtualization, may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment/misdirection techniques may also provide organizations additional time to successfully perform core missions and business functions. Because of the time and effort required to support concealment/misdirection techniques, it is anticipated that such techniques would be used by organizations on a very limited basis.

SC-30 Compliance Description:

SC-32 – Information System Partitioning

CMS ARS Mod 2.0 - Control:
The organization partitions the information system into defined information system components (defined in the applicable security plan) residing in separate physical domains or environments based on defined circumstances (defined in the applicable security plan) for physical separation of components.

Guidance
Information system partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the more critical components, to more significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components.

SC-32 Compliance Description:

SC-39 – Process Isolation

CMS ARS Mod 2.0 - Control:
The information system maintains a separate execution domain for each executing process.

Guidance
Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies.

SC-39 Compliance Description:

SC-CMS-1 – Electronic Mail

CMS ARS Mod 2.0 - Control:
Controls shall be implemented to protect sensitive information that is sent via email.

Implementation Standard(s)
1. Prior to sending an email, place all sensitive information in an encrypted attachment.

Guidance
A good place to obtain recommended security practices for handling sensitive information via e-mail is NIST SP 800-45 (as amended), Guidelines on Electronic Mail Security.

SC-CMS-1 Compliance Description:

SC-CMS-2 – Website Usage

CMS ARS Mod 2.0 - Control:
Web sites are operated within the restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and HHS directives and instruction.

Guidance
Monitor the CMS and DHHS security programs to determine if there are any modified directives and instruction.

SC-CMS-2 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

System and Information Integrity (SI) Controls

SI-1 – System and Information Integrity Policy and Procedures

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
b. Reviews and updates (as necessary) the current:
1. System and information integrity policy within every three hundred sixty-five (365) days; and
2. System and information integrity procedures within every three hundred sixty-five (365) days.

Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

SI-1 Compliance Description:

SI-2 – Flaw Remediation

CMS ARS Mod 2.0 - Control:
The organization:
a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates as directed in Implementation Standard 1; and
d. Incorporates flaw remediation into the organizational configuration management process.

Implementation Standard(s)
1. Correct identified security-related information system flaws on production equipment within ten (10) business days and all others within thirty (30) calendar days.
(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes, and
(b) Manage the flaw remediation process centrally.
2. A risk-based decision is documented through the configuration management process in the form of written authorization from the CMS CIO or his/her designated representative (e.g., the system data owner or CMS CISO) if a security patch is not applied to a security-based system or network.

Guidance
Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, and hot fixes. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

SI-2 Compliance Description:

SI-2(1) - Central Management – Enhancement

CMS ARS Mod 2.0 - Control:
The organization centrally manages the flaw remediation process.

Guidance
Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls.

SI-2(1) Compliance Description:

SI-2(2) - Automated Flaw Remediation Status – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.

Guidance
None

SI-2(2) Compliance Description:

SI-3 – Malicious Code Protection

CMS ARS Mod 2.0 - Control:
The organization:
a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Updates malicious code protection mechanisms whenever new releases are available in accordance with CMS configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
1. Perform periodic scans of the information system using the frequency specified in Implementation Standard 1, and real-time scans of files from external sources at endpoint, and/or network entry/exit points, as the files are downloaded, opened, or executed in accordance with organizational security policy; and
2. Block and quarantine malicious code and send alert to administrator in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Implementation Standard(s)
1. Desktop malicious code scanning software is configured to perform critical system file scans every twenty-four (24) hours.
2. **(For CSP only)** For service providers, the organization configures malicious code protection mechanisms to:
- Perform periodic scans of the information system at least weekly and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
- Block or quarantine malicious code, send alert to administrator, send alert to FedRAMP in response to malicious code detection.

Guidance
Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files.

SI-3 Compliance Description:

SI-3(1) - Central Management – Enhancement

CMS ARS Mod 2.0 - Control:
The organization centrally manages malicious code protection mechanisms.

Guidance
Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls.

SI-3(1) Compliance Description:

SI-3(2) - Automatic Updates – Enhancement

CMS ARS Mod 2.0 - Control:
The information system automatically updates malicious code protection mechanisms.

Guidance
Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

SI-3(2) Compliance Description:

SI-4 – Information System Monitoring

CMS ARS Mod 2.0 - Control:
The organization:
a. Monitors the information system to detect:
1. Attacks and indicators of potential attacks in accordance with the current Risk Management Handbook (RMH), Volume II, Procedure 7.2, Incident Handling ; and
2. Unauthorized local, network, and remote connections;
b. Identifies unauthorized use of the information system through defined techniques and methods (defined in the applicable security plan);
c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations;
and
g. Provides defined information system monitoring information (defined in the applicable security plan) to defined personnel or roles (defined in the applicable security plan) as needed, and at defined frequency (defined in the applicable security plan).

Implementation Standard(s)
1. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.
2. **(For CSP only)** For service providers, the organization monitors events on the information system to ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examines system records to confirm that the system is functioning in an optimal, resilient, and secure state; identifies irregularities or anomalies that are indicators of a system malfunction or compromise; and detects information system attacks.
3. **(For CSP only)** For service providers, the organization monitors for unauthorized remote connections to the information system continuously, real time, and takes appropriate action if an unauthorized connection is discovered.

Guidance
Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to
support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

SI-4 Compliance Description:

SI-4(1) - System-Wide Intrusion Detection System – Enhancement

CMS ARS Mod 2.0 - Control:
The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

Guidance
None

SI-4(1) Compliance Description:

SI-4(2) - Automated Tools for Real-Time Analysis – Enhancement

CMS ARS Mod 2.0 - Control:
The organization employs automated tools to support near real-time analysis of events.

Guidance
Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.

SI-4(2) Compliance Description:

SI-4(4) - Inbound and Outbound Communications Traffic – Enhancement

CMS ARS Mod 2.0 - Control:
The information system monitors inbound and outbound communications traffic at a defined frequency (defined in the applicable security plan) for unusual or unauthorized
activities or conditions.

Guidance
Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.

SI-4(4) Compliance Description:

SI-4(5) - System-Generated Alerts – Enhancement

CMS ARS Mod 2.0 - Control:
The information system alerts to defined personnel or roles (defined in the applicable security plan) when the following indications of compromise or potential compromise occur:
(a) Presence of malicious code,
(b) Unauthorized export of information,
(c) Signaling to an external information system, or
(d) Potential intrusions.

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Enhancement. The indications that a compromise or potential compromise occurred include: protected information system files or directories have been modified without notification from the appropriate change/configuration management channels; information system performance indicates resource consumption that is inconsistent with expected operating conditions; auditing functionality has been disabled or modified to reduce audit visibility; audit or log records have been deleted or modified without explanation; information system is raising alerts or faults in a manner that indicates the presence of an abnormal condition; resource or service requests are initiated from clients that are outside of the expected client membership set; information system reports failed logins or password changes for administrative or key service accounts; processes and services are running that are outside of the baseline system profile; utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose.
2. **(For CSP only)** For service providers, the organization defines additional compromise indicators as needed.

Guidance
Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers.
(For CSP only) Alerts may be generated from a variety of sources including but not limited to malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

SI-4(5) Compliance Description:

SI-5 – Security Alerts, Advisories, and Directives

CMS ARS Mod 2.0 - Control:
The organization:
a. Receives information system security alerts, advisories, and directives from defined external organizations (defined in the applicable security plan) on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to: defined personnel or roles (defined in the applicable security plan); and
d. Implements security directives in accordance with established time frames, or notifies CMS of the degree of noncompliance.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization disseminates security alerts, advisories, and directives to all staff with system administration, monitoring, and/or security responsibilities including but not limited to FedRAMP.
2. **(For CSP only)** For service providers, the organization defines a list of personnel (identified by name and/or by role) with system administration, monitoring, and/or security responsibilities who are to receive security alerts, advisories, and directives. The list also includes designated FedRAMP personnel.

Guidance
The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.

SI-5 Compliance Description:

SI-6 – Security Function Verification

CMS ARS Mod 2.0 - Control:
(For CSP only) The information system:
a. Verifies the correct operation of defined security functions (defined in the applicable security plan);
b. Performs this verification upon system startup and restart; upon command by user with appropriate privilege periodically on a monthly basis;
c. Notifies system administration of failed security verification tests; and
d. Shuts the information system down, or restarts the information system, or performs some other defined alternative action(s) (defined in the applicable security plan) when anomalies are discovered.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the information system verifies the correct operation of security functions upon system startup and/or restart and periodically every ninety (90) days, and notifies system administrator and performs FedRAMP-defined actions when anomalies are discovered.

Guidance
(For CSP only) Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights.

SI-6 Compliance Description:

SI-7 – Software, Firmware, and Information Integrity

CMS ARS Mod 2.0 - Control:
The organization employs integrity verification tools to detect unauthorized changes to software and information.

Guidance
Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.

SI-7 Compliance Description:

SI-7(1) - Integrity Checks – Enhancement

CMS ARS Mod 2.0 - Control:
The information system performs an integrity check of software and information daily.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization reassesses the integrity of software and information by performing at least monthly scans of the information system.

Guidance
Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.

SI-7(1) Compliance Description:

SI-7(7) - Integration of Detection and Response – Enhancement

CMS ARS Mod 2.0 - Control:
The organization incorporates the detection of unauthorized defined security-relevant changes (defined in the applicable security plan) to the information system into the organizational incident response capability.

Guidance
This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges.

SI-7(7) Compliance Description:

SI-8 – Spam Protection

CMS ARS Mod 2.0 - Control:
The organization:
a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Implementation Standard(s)
1. **(For CSP only)** For service providers, the organization:
a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Guidance
Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions.

SI-8 Compliance Description:

SI-8(1) - Central Management – Enhancement

CMS ARS Mod 2.0 - Control:
The organization centrally manages spam protection mechanisms.

Guidance
Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls.

SI-8(1) Compliance Description:

SI-8(2) - Automatic Updates – Enhancement

CMS ARS Mod 2.0 - Control:
The information system automatically updates spam protection mechanisms.

Guidance
None

SI-8(2) Compliance Description:

SI-10 – Information Input Validation

CMS ARS Mod 2.0 - Control:
The information system checks the validity of defined information inputs (defined in the applicable security plan) for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.

Guidance
Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

SI-10 Compliance Description:

SI-11 – Error Handling

CMS ARS Mod 2.0 - Control:
The information system:
a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
b. Reveals error messages only to defined personnel or roles (defined in the applicable security plan).

Implementation Standard(s)
1. **(For CSP only)** For service providers, this Standard replaces the above Control. The information system generates error messages that provide information necessary for corrective actions without revealing user name and password combinations; attributes used to validate a password reset request (e.g. security questions); personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record); biometric data or personal characteristics used to authenticate identity; sensitive financial records (e.g. account numbers, access codes); content related to internal security functions (i.e., private encryption keys, white list or blacklist rules, object permission attributes and settings in error logs and administrative messages that could be exploited by adversaries.

Guidance
Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information.

SI-11 Compliance Description:

SI-12 – Information Handling and Retention

CMS ARS Mod 2.0 - Control:
The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Implementation Standard(s)
1. Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with CMS policy and all applicable National Archives and Records Administration (NARA) requirements.

SI-12 – Information Handling and Retention (Moderate) P2
Control
The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
Implementation Standard(s)
1. Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with CMS policy and all applicable National Archives and Records Administration (NARA) requirements.
Guidance
Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention.

SI-12 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Program Management (PM) Controls

PM-1 – Information Security Program Plan

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops and disseminates an organization-wide information security program plan that:
1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
b. Reviews the organization-wide information security program plan within every three hundred sixty-five (365) days;
c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
d. Protects the information security program plan from unauthorized disclosure and modification.

Guidance
Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls. Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems.

PM-1 Compliance Description:

PM-2 – Senior Information Security Officer

CMS ARS Mod 2.0 - Control:
The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Guidance
The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.

PM-2 Compliance Description:

PM-3 – Information Security Resources

CMS ARS Mod 2.0 - Control:
The organization:
a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and
c. Ensures that information security resources are available for expenditure as planned.

Guidance
Organizations consider establishing champions for information security efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process.

PM-3 Compliance Description:

PM-4 – Plan of Action and Milestones Process

CMS ARS Mod 2.0 - Control:
The organization:
a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
1. Are developed and maintained;
2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
3. Are reported in accordance with OMB FISMA reporting requirements.
b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Guidance
The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information system), organizations view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from security control assessments and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.

PM-4 Compliance Description:

PM-5 – Information System Inventory

CMS ARS Mod 2.0 - Control:
The organization develops and maintains an inventory of its information systems.

Guidance
This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements. For specific information system inventory reporting requirements, organizations consult OMB annual FISMA reporting guidance.

PM-5 Compliance Description:

PM-6 – Information Security Measures of Performance

CMS ARS Mod 2.0 - Control:
The organization develops, monitors, and reports on the results of information security measures of performance.

Guidance
Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

PM-6 Compliance Description:

PM-7 – Enterprise Architecture

CMS ARS Mod 2.0 - Control:
The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Guidance
The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This process of security requirements integration also embeds into the enterprise architecture, an integral information security architecture consistent with organizational risk management and information security strategies. For PM-7, the information security architecture is developed at a system-of-systems level (organization-wide), representing all of the organizational information systems. For PL-8, the information security architecture is developed at a level representing an individual information system but at the same time, is consistent with the information security architecture defined for the organization. Security requirements and security control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures.

PM-7 Compliance Description:

PM-8 – Critical Infrastructure Plan

CMS ARS Mod 2.0 - Control:
The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Guidance
Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

PM-8 Compliance Description:

PM-9 – Risk Management Strategy

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
b. Implements the risk management strategy consistently across the organization; and
c. Reviews and updates the risk management strategy as required, to address organizational changes.

Guidance
An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive.

PM-9 Compliance Description:

PM-10 – Security Authorization Process

CMS ARS Mod 2.0 - Control:
The organization:
a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes;
b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
c. Fully integrates the security authorization processes into an organization-wide risk management program.

Guidance
Security authorization processes for information systems and environments of operation require the implementation of an organization-wide risk management process, a Risk Management Framework, and associated security standards and guidelines. Specific roles within the risk management process include an organizational risk executive (function) and designated authorizing officials for each organizational information system and common control provider. Security authorization processes are integrated with organizational continuous monitoring processes to facilitate ongoing understanding and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation.

PM-10 Compliance Description:

PM-11 – Mission/Business Process Definition

CMS ARS Mod 2.0 - Control:
The organization:
a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and
b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

Guidance
Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure.

PM-11 Compliance Description:

PM-12 – Insider Threat Program

CMS ARS Mod 2.0 - Control:
The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

Guidance
Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior organizational official is designated by the department/agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs as a minimum, prepare department/agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on governmentowned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis, and conduct selfassessments of department/agency insider threat posture. Insider threat programs can leverage the existence of incident handling teams organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines.

PM-12 Compliance Description:

PM-13 – Information Security Workforce

CMS ARS Mod 2.0 - Control:
The organization establishes an information security workforce development and improvement program.

Guidance
Information security workforce development and improvement programs include, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs can also include associated information security career paths to encourage: (i) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals.

PM-13 Compliance Description:

PM-14 – Testing, Training, and Monitoring

CMS ARS Mod 2.0 - Control:
The organization:
a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:
1. Are developed and maintained; and
2. Continue to be executed in a timely manner;
b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Guidance
This control ensures that organizations provide oversight for the security testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the importance of continuous monitoring programs, the implementation of information security across the three tiers of the risk management hierarchy, and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security controls. Security training activities, while typically focused on individual information systems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

PM-14 Compliance Description:

PM-15 – Contacts with Security Groups and Associations

CMS ARS Mod 2.0 - Control:
The organization establishes and institutionalizes contact with selected groups and associations within the security community:
a. To facilitate ongoing security education and training for organizational personnel;
b. To maintain currency with recommended security practices, techniques, and technologies; and
c. To share current security-related information including threats, vulnerabilities, and incidents.

Guidance
Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

PM-15 Compliance Description:

PM-16 – Threat Awareness Program

CMS ARS Mod 2.0 - Control:
The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

Guidance
Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.

PM-16 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Authority and Purpose (AP) Controls

AP-1 – Authority to Collect

CMS ARS Mod 2.0 - Control:
The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.

Guidance
Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements.

AP-1 Compliance Description:

AP-2 – Purpose Specification

CMS ARS Mod 2.0 - Control:
The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

Guidance
Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII). Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice.

AP-2 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Accountability, Audit, and Risk Management (AR) Controls

AR-1 – Governance and Privacy Program

CMS ARS Mod 2.0 - Control:

AR-1 – Governance and Privacy Program (Moderate) P1
Control
The organization:
a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems;
b. Monitors federal privacy laws and policy for changes that affect the privacy program;
c. Allocates an appropriate allocation of budget and staffing resources to implement and operate the organization-wide privacy program;
d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;
e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and
f. Updates privacy plan, policies, and procedures, as required to address changing requirements, but at least biennially.
Guidance
The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of an SAOP/CPO with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SAOP/CPO, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development, implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls.
To further accountability, the SAOP/CPO develops privacy plans to document the privacy requirements of organizations and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of organizational privacy operations and supports resource requests by the SAOP/CPO. A single plan or multiple plans may be necessary depending upon the organizational structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as Privacy Impact Assessments (PIA) and System of Records Notices (SORN). A comprehensive plan may include a baseline of privacy controls selected from this appendix and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating

Guidance
The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of an SAOP/CPO with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SAOP/CPO, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development, implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls.
To further accountability, the SAOP/CPO develops privacy plans to document the privacy requirements of organizations and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of organizational privacy operations and supports resource requests by the SAOP/CPO. A single plan or multiple plans may be necessary depending upon the organizational structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as Privacy Impact Assessments (PIA) and System of Records Notices (SORN). A comprehensive plan may include a baseline of privacy controls selected from this appendix and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls.

AR-1 Compliance Description:

AR-2 – Privacy Impact and Risk Assessment

CMS ARS Mod 2.0 - Control:
The organization:
a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and
b. Conducts Privacy Impact Assessments (PIA) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Guidance
Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. They include, but are not limited to, the conduct of PIAs. The PIA is both a process and the document that is the outcome of that process. OMB Memorandum 03-22 provides guidance to organizations for implementing the privacy provisions of the E-Government Act of 2002, including guidance on when PIAs are required for information systems. Some organizations may be required by law or policy to extend the PIA requirement to other activities involving PII or otherwise impacting privacy (e.g., programs, projects, or regulations). PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information systems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public of privacy practices. PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.

AR-2 Compliance Description:

AR-3 – Privacy Requirements for Contractors and Service Providers

CMS ARS Mod 2.0 - Control:
The organization:
a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and
b. Includes privacy requirements in contracts and other acquisition-related documents.

Guidance
Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control.

AR-3 Compliance Description:

AR-4 – Privacy Monitoring and Auditing

CMS ARS Mod 2.0 - Control:
The organization monitors and audits privacy controls and internal privacy policy as required to ensure effective implementation.

Guidance
To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems. In addition to auditing for effective implementation of all privacy controls identified in [800-53 Appendix J], organizations assess whether they: (i) implement a process to embed privacy considerations into the life cycle of personally identifiable information (PII), programs, information systems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations, and policies; (iii) track programs, information systems, and applications that collect and maintain PII to ensure compliance; (iv) ensure that access to PII is only on a need-to-know basis; and (v) ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s).
Organizations also: (i) implement technology to audit for the security, appropriate use, and loss of PII; (ii) perform reviews to ensure physical security of documents containing PII; (iii) assess contractor compliance with privacy requirements; and (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials.

AR-4 Compliance Description:

AR-5 – Privacy Awareness and Training

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;
b. Administers basic privacy training at within every three hundred sixty-five (365) days, and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII within every three hundred sixty-five (365) days; and
c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements within every three hundred sixty-five (365) days.

Guidance
Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act of 2002 and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use requirements identified in public notices, such as Privacy Impact Assessments (PIA) or System of Records Notices (SORN) for a program or information system. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program websites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors. Organizations update training based on changing statutory, regulatory, mission, program, business process, and information system requirements, or on the results of compliance monitoring and auditing. Where appropriate, organizations may provide privacy training as part of existing information security training.

AR-5 Compliance Description:

AR-6 – Privacy Reporting

CMS ARS Mod 2.0 - Control:
The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Guidance
Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Types of privacy reports include: (i) annual Senior Agency Official for Privacy (SAOP) reports to OMB; (ii) reports to Congress required by the Implementing Regulations of the 9/11 Commission Act; or (iii) other public reports required by specific statutory mandates or internal policies of organizations. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

AR-6 Compliance Description:

AR-7 – Privacy-Enhanced System Design and Development

CMS ARS Mod 2.0 - Control:
The organization designs information systems to support privacy by automating privacy controls.

Guidance
To the extent feasible, when designing organizational information systems, organizations employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, organizations mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents. Organizations also conduct periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act and the organization's privacy policy. Regardless of whether automated privacy controls are employed, organizations regularly monitor information system use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notice of organizations, or in a manner compatible with those purposes.

AR-7 Compliance Description:

AR-8 – Accounting of Disclosures

CMS ARS Mod 2.0 - Control:
The organization:
a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:
(1) Date, nature, and purpose of each disclosure of a record; and
(2) Name and address of the person or agency to which the disclosure was made;
b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and
c. Makes the accounting of disclosures available to the person named in the record upon request.

Guidance
The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) periodically consults with managers of organization systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.

AR-8 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Data Quality and Integrity (DI) Controls

DI-1 – Data Quality

CMS ARS Mod 2.0 - Control:
The organization:
a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;
b. Collects PII directly from the individual to the greatest extent practicable;
c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems as directed by the Data Integrity Board; and
d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Guidance
Organizations take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.
When PII is of a sufficiently sensitive nature (e.g., when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit), organizations incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated.

DI-1 Compliance Description:

DI-1(1) - Validate PII – Enhancement

CMS ARS Mod 2.0 - Control:
The organization requests that the individual or individual's authorized representative validate PII during the collection process.

Guidance
None

DI-1(1) Compliance Description:

DI-1(2) - Re-Validate PII – Enhancement

CMS ARS Mod 2.0 - Control:
The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate as directed by the Data Integrity Board.

Guidance
None

DI-1(2) Compliance Description:

DI-2 – Data Integrity and Data Integrity Board

CMS ARS Mod 2.0 - Control:
The organization:
a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and
b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

Guidance
Organizations conducting or participating in Computer Matching Agreements with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. In many organizations, the Data Integrity Board is led by the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO). The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under Computer Matching Agreements.

DI-2 Compliance Description:

DI-2(1) - Publish Agreements on Website – Enhancement

CMS ARS Mod 2.0 - Control:
The organization publishes Computer Matching Agreements on its public website.

Guidance
None

DI-2(1) Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Data Minimization and Retention (DM) Controls

DM-1 – Minimization of Personally Identifiable Information

CMS ARS Mod 2.0 - Control:
The organization:
a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and
c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings, within every three hundred sixty-five (365) days, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Guidance
Organizations take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose.
Organizations can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. OMB Memorandum 07-16 requires organizations to conduct both an initial review and subsequent reviews of their holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Organizations are also directed by OMB to reduce their holdings to the minimum necessary for the proper performance of a documented organizational business purpose. OMB Memorandum 07-16 requires organizations to develop and publicize, either through a notice in the Federal Register or on their websites, a schedule for periodic reviews of their holdings to supplement the initial review. Organizations coordinate with their federal records officers to ensure that reductions in organizational holdings of PII are consistent with NARA retention schedules.
By performing periodic evaluations, organizations reduce risk, ensure that they are collecting only the data specified in the notice, and ensure that the data collected is still relevant and necessary for the purpose(s) specified in the notice.

DM-1 Compliance Description:

DM-1(1) - Locate/Remove/Redact/Anonymize PII – Enhancement

CMS ARS Mod 2.0 - Control:
The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

Guidance
NIST Special Publication 800-122 provides guidance on anonymization.

DM-1(1) Compliance Description:

DM-2 – Data Retention and Disposal

CMS ARS Mod 2.0 - Control:
The organization:
a. Retains each collection of personally identifiable information (PII) for minimum allowable necessary to fulfill the purpose(s) identified in the notice or as required by law;
b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
c. Uses legally compliant techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Guidance
NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper.
Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII.
Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche may not permit the removal of individual records without the destruction of the entire database contained on such media.

DM-2 Compliance Description:

DM-2(1) - System Configuration – Enhancement

CMS ARS Mod 2.0 - Control:
The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

Guidance
None

DM-2(1) Compliance Description:

DM-3 – Minimization of PII Used in Testing, Training, and Research

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and
b. Implements controls to protect PII used for testing, training, and research.

Guidance
Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. Organizations consult with the SAOP/CPO and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected.

DM-3 Compliance Description:

DM-3(1) - Risk Minimization Techniques – Enhancement

CMS ARS Mod 2.0 - Control:
The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

Guidance
Organizations can minimize risk to privacy of PII by using techniques such as de-identification.

DM-3(1) Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Individual Participation and Redress (IP) Controls

IP-1 – Consent

CMS ARS Mod 2.0 - Control:
The organization:
a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;
b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and
d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Guidance
Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices.
Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow organizations to collect or use PII. For example, opt-in consent may require an individual to click a radio button on a website, or sign a document providing consent. In contrast, opt-out requires individuals to take action to prevent the new or continued collection or use of such PII. For example, the Federal Trade Commission's Do-Not-Call Registry allows individuals to opt-out of receiving unsolicited telemarketing calls by requesting to be added to a list. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. Organizational consent mechanisms include a discussion of the consequences to individuals of failure to provide PII. Consequences can vary from organization to organization.

IP-1 Compliance Description:

IP-1(1) - Mechanisms Supporting Itemized or Tiered Consent – Enhancement

CMS ARS Mod 2.0 - Control:
The organization implements mechanisms to support itemized or tiered consent for specific uses of data.

Guidance
Organizations can provide, for example, individuals' itemized choices as to whether they wish to be contacted for any of a variety of purposes. In this situation, organizations construct consent mechanisms to ensure that organizational operations comply with individual choices.

IP-1(1) Compliance Description:

IP-2 – Individual Access

CMS ARS Mod 2.0 - Control:
The organization:
a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;
b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;
c. Publishes access procedures in System of Records Notices (SORNs); and
d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Guidance
Access affords individuals the ability to review PII about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Access to certain types of records may not be appropriate, however, and heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act. In addition, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding.

IP-2 Compliance Description:

IP-3 – Redress

CMS ARS Mod 2.0 - Control:
The organization:
a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and
b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

Guidance
Redress supports the ability of individuals to ensure the accuracy of PII held by organizations. Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate.
To provide effective redress, organizations: (i) provide effective notice of the existence of a PII collection; (ii) provide plain language explanations of the processes and mechanisms for requesting access to records; (iii) establish criteria for submitting requests for correction or amendment; (iv) implement resources to analyze and adjudicate requests; (v) implement means of correcting or amending data collections; and (vi) review any decisions that may have been the result of inaccurate information. Organizational redress processes provide responses to individuals of decisions to deny requests for correction or amendment, including the reasons for those decisions, a means to record individual objections to the organizational decisions, and a means of requesting organizational reviews of the initial determinations. Where PII is corrected or amended, organizations take steps to ensure that all authorized recipients of that PII are informed of the corrected or amended information. In instances where redress involves information obtained from other organizations, redress processes include coordination with organizations that originally collected the information.

IP-3 Compliance Description:

IP-4 – Complaint Management

CMS ARS Mod 2.0 - Control:
The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Guidance
Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards. Organizations provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) or other official designated to receive complaints), and are easy to use. Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner.

IP-4 Compliance Description:

IP-4(1) - Response Times – Enhancement

CMS ARS Mod 2.0 - Control:
The organization responds to complaints, concerns, or questions from individuals within the CMS-defined time period.

Guidance
None

IP-4(1) Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Security (SE) Controls

SE-1 – Inventory of Personally Identifiable Information

CMS ARS Mod 2.0 - Control:
The organization:
a. Establishes, maintains, and updates, within every three hundred sixty-five (365) days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and
b. Provides each update of the PII inventory to the Senior Official for Privacy and the Chief information Security Officer to support the establishment of information security requirements for all new or modified information systems containing PII.

Guidance
The PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII consistent with NIST 800-53 Appendix F, and to mitigate risks of PII exposure. As one method of gathering information for their PII inventories, organizations may extract the following information elements from Privacy Impact Assessments (PIA) for information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Organizations take due care in updating the inventories by identifying linkable data that could create PII.

SE-1 Compliance Description:

SE-2 – Privacy Incident Response

CMS ARS Mod 2.0 - Control:
The organization:
a. Develops and implements a Privacy Incident Response Plan; and
b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

Guidance
In contrast to the Incident Response (IR) family in NIST 800-53 Appendix F, which concerns a broader range of incidents affecting information security, this control uses the term Privacy Incident to describe only those incidents that relate to personally identifiable information (PII). The organization Privacy Incident Response Plan is developed under the leadership of the SAOP/CPO. The plan includes: (i) the establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan; (ii) a process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly; (iii) a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; (iv) internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), consistent with organizational incident management structures; and (v) internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials. Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a breach. Organizations may also choose to integrate Privacy Incident Response Plans with Security Incident Response Plans, or keep the plans separate.

SE-2 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Transparency (TR) Controls

TR-1 – Privacy Notice

CMS ARS Mod 2.0 - Control:
The organization:
a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;
b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and
c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Guidance
Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices. The organization may provide general public notice through a variety of means, as required by law or policy, including System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), or in a website privacy policy. As required by the Privacy Act, the organization also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.
The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of the organization's public notices, in consultation with legal counsel and relevant program managers. The public notice requirement in this control is satisfied by an organization's compliance with the public notice provisions of the Privacy Act, the E-Government Act's PIA requirement, with OMB guidance related to federal agency privacy notices, and, where applicable, with policy pertaining to participation in the Information Sharing Environment (ISE). Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SAOP/CPO and counsel.

TR-1 Compliance Description:

TR-1(1) - Real-Time or Layered Notice – Enhancement

CMS ARS Mod 2.0 - Control:
The organization provides real-time and/or layered notice when it collects PII.

Guidance
Real-time notice is defined as notice at the point of collection. A layered notice approach involves providing individuals with a summary of key points in the organization's privacy policy. A second notice provides more detailed/specific information.

TR-1(1) Compliance Description:

TR-2 – System of Records Notices and Privacy Act Statements

CMS ARS Mod 2.0 - Control:
The organization:
a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);
b. Keeps SORNs current; and
c. Includes Privacy Act Statements on it s forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

Guidance
Organizations issue SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as "a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier." SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. Privacy Act Statements provide notice of: (i) the authority of organizations to collect PII; (ii) whether providing PII is mandatory or optional; (iii) the principal purpose(s) for which the PII is to be used; (iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information requested. When information is collected verbally, organizations read a Privacy Act Statement prior to initiating the collection of PII (for example, when conducting telephone interviews or surveys).

TR-2 Compliance Description:

TR-2(1) - Public Website Publication – Enhancement

CMS ARS Mod 2.0 - Control:
The organization publishes SORNs on its public website.

Guidance
None

TR-2(1) Compliance Description:

TR-3 – Dissemination of Privacy Program Information

CMS ARS Mod 2.0 - Control:
The organization:
a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and
b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Guidance
Organizations employ different mechanisms for informing the public about their privacy practices including, but not limited to, Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). Organizations also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

TR-3 Compliance Description:

(QE's Company Name Here)

SECURITY CONTROLS DETAIL AND COMMENT

Use Limitation (UL) Controls

UL-1 – Internal Use

CMS ARS Mod 2.0 - Control:
The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Guidance
Organizations take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII. With guidance from the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and where appropriate, legal counsel, organizations document processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new use(s) of PII.

UL-1 Compliance Description:

UL-2 – Information Sharing with Third Parties

CMS ARS Mod 2.0 - Control:
The organization:
a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or in a manner compatible with those purposes;
b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;
c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and
d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Guidance
The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act and/or specified in a notice, organizations evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, organizations review, update, and republish their Privacy Impact Assessments (PIA), System of Records Notices (SORN), website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared.

UL-2 Compliance Description: