Defense Security Service
Industrial Security Field Operations
National Industrial Security Program Authorization Office

Assessment and Authorization Process Manual

Version 1.0

August 24, 2016

EXECUTIVE SUMMARY

The policy of the U.S. Government is that all classified information must be appropriately safeguarded to assure the confidentiality of that information, as well as the integrity and availability of that information when required by contract. This Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM) is intended for use by cleared contractors participating in the National Industrial Security Program. It provides standardized security policies and procedures for use in safeguarding classified information processed by contractors' information systems (ISs) that operate under the security cognizance of the Defense Security Service.

Federal agencies, to include the DoD, Special Access Program (SAP), and Intelligence communities, are adopting common guidelines to streamline and build reciprocity into the assessment and authorization process (formerly known as Certification and Accreditation (C&A)). The DAAPM transitions DSS Certification and Accreditation processes to the Risk Management Framework (RMF) made applicable to cleared contractors by DoD 5220.22-M, Change 2, *National Industrial Security Program Operating Manual (NISPOM), issued on May 18, 2016*. The DAAPM is based on the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-37, *Risk Management Framework*, and SP 800-53, Version 4, *Security and Privacy Controls for Federal ISs*, and the Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems* and CNSSD 504, *Directive on Protecting national Security Systems From Insider Threat*.

The DAAPM also incorporates Insider Threat minimum requirements defined in the NISPOM, which are consistent with the requirements of Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing of Classified Information,* and the Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Threat Programs*.

This process manual is not intended, does not, and may not be relied upon or construed to create any right or benefit, substantive or procedural, enforceable at law against the United States, its agencies, officers or employees. The Federal Government reserves the right, and has the obligation, to impose any security method, safeguard, or restriction it believes necessary to verify that unauthorized access to classified information is effectively precluded and that performance of classified contracts is not adversely affected.

TABLE OF CONTENTS

1   INTRODUCTION

1.1 BACKGROUND

Federal agencies are adopting the NIST RMF as a common set of guidelines for the assessment and authorization of ISs. In an effort to streamline and build reciprocity into the DSS processes, DSS is adopting these standards, as well, to support the authorization of contractor's Information Systems (ISs) processing classified information as part of the NISP. The RMF focuses on a more holistic and strategic process for the risk management of information systems, and on processes and procedures designed to develop trust across the Federal Government. Implementation of the RMF provides organizations with a disciplined, structured, flexible, and repeatable process for managing risk related to the operation and use of ISs.

To enable information sharing within the Federal Government, the CNSS directives and instructions establish standards for IS security categorization, security controls selection, and security controls assessment and monitoring for consistency and reciprocity. The DSS is ensuring that its policies and procedures comply with these standards allowing NISP contractors to align with the Federal Government's approach for IS security.

In addition to the Process Manual, key documents supporting the assessment and authorization of classified ISs under DSS cognizance include:
- DoD 5220.22-M Change-2, *National Industrial Security Program Operating Manual (NISPOM)*
- NIST Special Publications (SP) Joint Task Force (JTF) Initiative documents:
  - NIST SP 800-53, Rev 4, *Recommended Security Controls for Federal Information Systems and Organizations*
  - NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*
  - NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal ISs*
- CNSS Instruction (CNSSI) 1253, *Security Categorization and Control Selection for National Security Systems*
- CNSS Directive (CNSSD) 504, *Directive on Protecting national Security Systems From Insider Threat*

1.1.1 CHANGE MANAGEMENT PROCESS

The DAAPM is a living document, with each proposed change receiving individual consideration as to its implementation guidance and timelines. The DSS NISP Authorization Office (NAO) has overall responsibility for content management of the DAAPM; however, this is accomplished through a change management process involving one member from NISP Administration and Policy Analysis (NAPA), and an industry representative from the NISPPAC C&A WG. This group is referred to as the Configuration Management Team (CMT). Changes to the DAAPM must be aligned to, and consistent with, the NIST and CNSS processes for security of information systems processing classified information.

The CMT's purpose is to evaluate proposed changes, review existing implementation guidance, and develop implementation and transition guidance for NISP contractors under DSS cognizance. CMT members are responsible for collecting, prioritizing, and determining the priority of proposed changes from their respective communities. Topics for consideration

include, but are not limited to, security control requirements, implementation, testing, and validation; as well as, security assessment and system authorization processes.

The CMT conducts quarterly review boards to introduce new items for consideration; review previously identified proposals; and make final adjudication decisions on proposed changes to the Process Manual. As changes are accepted and implemented, the CMT lead annotates the details of the changes in the DAAPM change log, which is a permanent part of the DAAPM. CMT members may request ad-hoc meetings as required to address high priority issues, and items recognized by all parties as administrative in nature may be worked through email channels for immediate implementation upon CMT approval. The NAO has final approval authority for all changes to the DAAPM.

Understanding that the DAAPM is a living document, the final security related requirements for each information system (IS) are those identified in the DSS approved system security plan (SSP). DSS personnel use the SSP as the document from which to evaluate the system requirements during IS certification and accreditation efforts and security vulnerability assessments. The DAAPM and accompanying change log are made available on the DSS/NAO Website.

Generate	Evaluate	Authorize	Implement
•Users Submit change requests to CMT Reps.	•CMT Reps evaluate for initial acceptance. •CMT Rep submits to CMT Brd for review.	•CMT assesses and makes final determiniation.	•NAO incorporates into DAAPM.
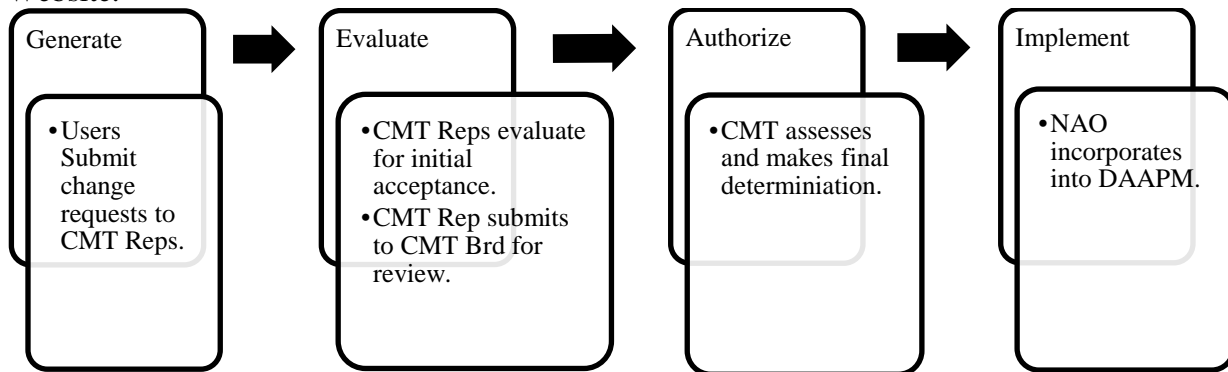
1.2 APPLICABILITY AND RECIPROCITY

Cleared contractors' IS which are used to process classified information under the NISP, and fall under the cognizance of DSS, will follow the guidance contained within this manual to complete the RMF process and obtain authorization for use. Special Access Systems (SAS) that fall under the cognizance of DSS will apply the DAAPM unless otherwise stated in the contract.

Reciprocity, as defined in CNSSI 4009, is a "Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse IS resources and/or to accept each other's assessed security posture in order to share information." This does not imply blind acceptance. The body of evidence used for assessments of the subject system will be provided to the other participant(s) who have a vested interest in establishing a mutual agreement. The receiving party will review the assessment evidence (system security plan (SSP), test plans, test procedures, test results, exceptions, etc.) and determine if there are any deltas in the evidence, e.g. baseline/overlay controls that were tailored, a test item that was omitted, etc. and identify items that may require negotiations.

Reciprocity means that the system(s) will not be retested or undergo another full assessment. In the spirit of reciprocity, the existing assessments will be accepted; only controls, test items or other pertinent items that were initially omitted are subject to evaluation/testing to assure the system meets any additional protections required for a successful reciprocal agreement.

1.3 REFERENCES
References pertaining to this document can be found in Appendix A. Additionally, references and resources applicable to a particular security topic can be found at the end of the section that addresses that topic.

1.4 CHANGES IN TERMINOLOGY
The below table provides a mapping between terms previously associated with C&A activities and new terms adopted under the Risk Management Framework.

Old Term	New Term
Certification and Accreditation (C&A) Process	Risk Management Framework (RMF)
Certification	Assessment or Security Control Assessment
Accreditation	Authorization
Requirements (Security or Identification and Authentication (IA))	Security Controls
Protection Level (PL)	Security Categorization
Level of Concern	Impact Level
Master System Security Plan (MSSP)/Self-Certification	MSSP/Type Authorization
IS Profile	System Security Plan (SSP)
Designated Approving Authority (DAA)	Authorizing Official (AO)
IS Security Professional (ISSP)	Security Control Assessor (SCA)/ISSP
Customer, Government Contracting Authority (GCA), etc.	Information Owner (IO)
Guest System	Federal Information System

2   ROLES AND RESPONSIBILITIES
The roles and responsibilities of the personnel involved with the RMF are summarized in the paragraphs below.

2.1 AUTHORIZING OFFICIAL
The AO is the senior official or executive with the authority to formally assume responsibility for operating an IS at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and national security.

Responsibilities of the AO include, but are not limited to:
a. Ensure each IS is properly assessed and authorized based on its environment of operation, security impact levels and required security controls;
b. Evaluate threats and vulnerabilities to ISs to ascertain the need for additional safeguards;
c. Issue security authorization decisions;
d. Ensure records are maintained for all IS authorizations under his/her purview;
e. Ensure IS security is an element of the life-cycle process;
f. Ensure advise and assistance related to the secure operation of IS is provided to contractor personnel as necessary;
g. Coordinate cyber incident responses related to classified ISs; and

h.   Reviews and approves Memorandum of Understanding or Agreements (MOU/A)/Interconnection Security Agreement (ISA) associated with IS processing classified information.

2.2 SECURITY CONTROL ASSESSOR
The SCA is an ISSP appointed by the AO to act on their behalf in the oversight of contractor IS processing classified information. The SCA is responsible for:
a. Conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an IS to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system).
b. Providing an assessment of the severity of weaknesses or deficiencies discovered in the IS and its environment of operation and recommend corrective actions to address identified vulnerabilities.
c. Providing advice and assistance, as needed by the contractor.
d. Advise the Information System Security Manager (ISSM) concerning the impact levels for Confidentiality, Integrity, and Availability for the information on a system;
e. Evaluate threats and vulnerabilities to ISs to ascertain the need for additional safeguards;
f. Ensure security assessments are completed for each IS;
g. At the conclusion of each security assessment activity, prepare the final Security Assessment Report (SAR) containing the results and vulnerabilities from the assessment;
h. Review POA&Ms to ensure identified weaknesses are identified in the POA&M, planned mitigation strategies and timelines are acceptable and on track, and provide recommendations to the AO regarding matters related to the POA&M;
i. Evaluate security assessment documentation and provide written recommendations for security authorization to the AO;
j. Develop recommendation for authorization and submit the security authorization package to the AO; and
k. Assess proposed changes to ISs, their environment of operation, and mission needs that could affect system authorization.

2.3 COMMON CONTROL PROVIDER (CCP)
A CCP is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by ISs). Responsibilities of the CCP include, but are not limited to:
a. Document the common controls in a SSP;
b. Ensure that required assessments of common controls are carried out as required;
c. Document assessment vulnerabilities in a SAR; and
d. Produce a POA&M for all security controls having weaknesses or deficiencies. SSPs, SARs, and POA&Ms associated with common controls will be made available to ISSMs inheriting those controls.

2.4 INFORMATION OWNER
An IO is an organizational official with statutory, management, or operational authority for specific information who has the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. The IO is a U.S. citizen and a government employee. Each respective GCA shall also serve as the IO. In information-sharing environments, the IO is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., DD Form 254 and security classification

guide) and retains that responsibility even when the information is shared with or provided to other organizations. Within the NISP, the owner/steward of the information processed, stored, or transmitted by an IS is not the same as the IS Owner. A single IS may contain information from multiple IOs. IOs provide input to IS Owners regarding:

a. Sensitivity of information under the Information System Owner's (ISO's) purview;
b. Signatory for the Risk Acknowledgement Letter (RAL);
c. Confidentiality, Integrity, and Availability impact levels associated with the IO's data when contractual requirements are higher than the baseline identified in NISPOM 8-301e(1)(2) or if concern is raised based on the Risk Assessment Report (RAR). (GCA concurrence is required whenever the categorization is raised from NISPOM baseline.);
d. Unique requirements for managing the IO's data (e.g., incident response, information contamination to other systems/media, and unique audit requirements); and
e. Whether foreign nationals may access the IO's data.

2.5 INFORMATION SYSTEM OWNER

An ISO is an organizational official, (i.e. GCA for government systems, the ISO for contractor owned systems oversees this role within the NISP) responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an IS. The ISO is responsible for addressing the operational interests of the user community (i.e., users who require access to the IS to satisfy mission, business, or operational requirements) and for ensuring compliance with information security requirements.

Responsibilities of the ISO include, but are not limited to:

a. Plan and budget for adequate on-site information security resources assigned to ISs under their purview;

2.6 INFORMATION SYSTEM SECURITY MANAGER

The contractor will appoint an ISSM who serves as a principal advisor on all matters, technical and otherwise, involving the security of ISs under his/her purview.
Responsibilities of an ISSM include, but are not limited to:

a. Develop and maintain an IS security program and policies for their assigned area of responsibility;
b. Develop and oversee operational ISs security implementation policy and guidelines;
c. Coordinate with SCA/AO on approval of Federal ISs;
d. The ISSM shall assign the ISSO.
e. Oversee Information System Security Officers (ISSOs) under their purview to ensure they follow established IS policies and procedures;
f. Monitor all available resources that provide warnings of system vulnerabilities or ongoing attacks and report them as necessary;
g. Ensure periodic testing is conducted to evaluate the security posture of IS;
h. If applicable, ensure all ISSOs receive the necessary technical and security training (e.g., operating system, networking, security management) to carry out their duties;
i. Ensure approved procedures are used for sanitizing and releasing system components and media;
j. Maintain a repository of all security authorizations for IS under their purview;
k. Coordinate IS security inspections, tests, and reviews;
l. Ensure proper measures are taken when an IS incident or vulnerability affecting classified systems or information is discovered;

m.   Ensure data ownership and responsibilities are established for each IS, and specific requirements (to include accountability, access and special handling requirements) are enforced;

n.   Ensure development and implementation of an effective IS security education, training, and awareness program;

o.   Ensure Configuration Management policies and procedures for authorizing the use of hardware/software on an IS are followed. Any additions, changes or modifications to hardware, software, or firmware must be coordinated with the ISSM/ISSO and appropriate AO prior to the addition, change or modification;

p.   Lead the Configuration Control Board (CCB), if applicable. The ISSM shall have authority to veto any proposed change they feel is detrimental to security. Appeals on an ISSM/ISSO veto may be taken to the AO. The ISSM may elect to delegate this responsibility to the ISSO;

q.   Maintain a working knowledge of system functions, security policies, technical security safeguards, and operational security measures;

r.   Manage, maintain, and execute the information security continuous monitoring (ISCM) plan;

s.   Ensure a Plan of action & Milestone (POA&M) is maintained for all security-related vulnerabilities and ensure serious or unresolved violations are reported to the AO;

t.   Assess changes to the system, its environment, and operational needs that could affect the security authorization;

u.   Coordinate with the contractor's Facility Security Officer (FSO) and the contractor's Insider Threat Program Senior Official (ITPSO) to ensure insider threat awareness is addressed within the contractor's IS programs;

v.   Ensures user activity monitoring data is analyzed, stored and protected in accordance with the ITPSO policies and procedures;

w.   Prepares and submits POA&Ms identifying IS weaknesses, mitigating actions, and the resources and timelines for corrective actions. Entries will be based on vulnerabilities and recommendations from the SAR, and Security Vulnerability Assessment (SVA);

x.   Be adequately trained and possess technical competence commensurate with the complexity of the ISs in addition to training identified in table "ISSM Required Training" within one year of appointment;

y.   Attend technical and security training (e.g., operating system, networking, security management) relative to assigned duties;

z.   Ensure compliance with current Information Assurance (IA) policies, concepts, and measures when designing, procuring, adopting, and developing new IS;

aa.   Ensure development and maintenance of the SSP and that the system is deployed and operated in accordance with the agreed-upon security controls;

bb.   Ensure enhancements to existing systems provide equal or improved security features and safeguards;

cc.   Ensure the Configuration Management (CM) process is addressed and used when new IS are under development, being procured, or delivered for operation. An integral part of the System Authorization process is CM. Therefore, it is imperative that AOs be advised of CM decisions;

dd.   Ensure a risk assessment is performed on the IS while under development and keep the risk assessment current throughout the acquisition/development portion of the life cycle;

ee.   Ensure security controls are implemented that protect the IS during development;

ff.   Evaluate interoperability with other systems;

gg.   Produce/develop security documentation (SSP, POA&M, Security Authorization Package, etc. as input to the Security Authorization Package);

hh.   Complete and coordinate a Security Assessment with the ISSO (if applicable);
ii.   Submit the Security Authorization Package to the AO/SCA for review and consideration;
jj.   Ensure the POA&M is initiated and submitted to the AO/SCA and is continually updated to reflect the current status of planned activities for correcting vulnerabilities associated with the required security controls and address any residual vulnerabilities;
kk.   Ensure all users have the requisite security clearances, authorization, need-to-know, and are aware of their security responsibilities before granting access to the IS;
      Report all security-related incidents;
ll.   Conduct periodic reviews of ISs to ensure compliance with the security authorization package;
mm.   Monitor system recovery processes to ensure security features and procedures are properly restored and functioning correctly;
nn.   Ensure all IS security-related documentation is current and accessible to properly authorized individuals;
oo.   Ensure audit records are collected and reviewed; and
pp.   Ensure the ISSO is adequately trained and possesses technical competence commensurate with the complexity of the ISs within one year of appointment.

ISSM Required Online Training
Categorization of the System (CS102.16)
Selecting Security Controls (CS103.16)
Implementation of Controls (CS104.16)
Assessing Security Controls (CS105.16)
Authorizing Systems (CS106.16)
Monitoring Security Controls (CS107.16)
Continuous Monitoring (CS200.16)
Completion of appropriate IT specific training (e.g., Security +, Microsoft, UNIX etc.)

2.7 INFORMATION SYSTEM SECURITY OFFICER

An ISSO is an individual responsible for ensuring the appropriate operational security posture is maintained for an IS and as such, works in close collaboration with the ISSM. The ISSO shall have the detailed knowledge and expertise required to manage the security aspects of an IS and, in many organizations, is assigned responsibility for the day-to-day security operations of a system. Responsibilities also include physical and environmental protection, personnel security, incident handling, and security training and awareness. In close coordination with the ISSM, the ISSO plays an active role in monitoring a system and its environment of operation to include developing and updating the SSP, managing and controlling changes to the system, and assessing the security impact of those changes.

Responsibilities of the ISSO include, but are not limited to:
a.   Ensure systems are operated, maintained, and disposed of in accordance with security policies and procedures as outlined in the security authorization package;
b.   Attend technical and security training (e.g., operating system, networking, security management) relative to assigned duties;
c.   Ensure all users have the requisite security clearances, authorization, need-to-know, and are aware of their security responsibilities before granting access to the IS;
d.   Report all security-related incidents to the ISSM;
e.   Conduct periodic reviews of ISs to ensure compliance with the security authorization package;

> f. Serve as member of the CCB, if designated by the ISSM;

g. Coordinate any changes or modifications to hardware, software, or firmware of a system with the ISSM prior to the change;

h. Formally notify the ISSM when changes occur that might affect system authorization;

i. Monitor system recovery processes to ensure security features and procedures are properly restored and functioning correctly;

j. Ensure all IS security-related documentation is current and accessible to properly authorized individuals;

k. Ensure audit records are collected and reviewed; and

l. ISSO shall be adequately trained and possesses technical competence commensurate with the complexity of the ISs.

Required Online Training
Categorization of the System (CS102.16)
Selecting Security Controls (CS103.16)
Implementation of Controls (CS104.16)
Assessing Security Controls (CS105.16)
Authorizing Systems (CS106.16)
Monitoring Security Controls (CS107.16)
Continuous Monitoring (CS200.16)
Completion of appropriate IT specific training (e.g., Security +, Microsoft, UNIX etc.)

2.8 PRIVILEGED USER ACCOUNTS

A privileged user account is provided to an individual who is authorized to perform security-relevant functions, such as system control, monitoring, data transfer, or administration functions that general users are not authorized to perform. See Account Management [AC-2], for privileged user responsibilities.

2.9 GENERAL USER ACCOUNTS

A general user account is provided to an individual who can receive information from, input information to, or modify information on a system. See Account Management [AC-2], for general user responsibilities.

3 RISK MANAGEMENT FRAMEWORK

3.1 INTRODUCTION TO THE RISK MANAGEMENT FRAMEWORK

NIST, in partnership with DoD, the Office of the Director of National Intelligence (ODNI), and CNSS, has developed a common information security framework for the federal government and its contractors. The intent of this common framework is to improve information security, strengthen risk management processes, and encourage reciprocity among federal agencies. NIST SP 800-37, developed by the JTF Transformation Initiative Working Group, transforms the traditional C&A process into the six-step RMF. The revised process emphasizes:

a. Building information security capabilities into federal IS through the application of community best practices for management, operational, and technical security controls;

b. Maintaining awareness of the security state of ISs on an ongoing basis through enhanced monitoring processes; and

c. Providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and national security arising from the operation and use of IS.

The RMF steps include:
   a. **Categorize** the IS and the information processed, stored, and transmitted by the system based on an analysis of the impact due to a loss of confidentiality, integrity and availability.
   b. **Select** an initial set of baseline security controls for the IS based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
   c. **Implement** the security controls and describe how the controls are employed within the IS and its environment of operation.
   d. **Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
   e. **Authorize** IS operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and national security resulting from the operation of the IS and the decision that this risk is acceptable.
   f. **Monitor** the security controls in the IS on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.
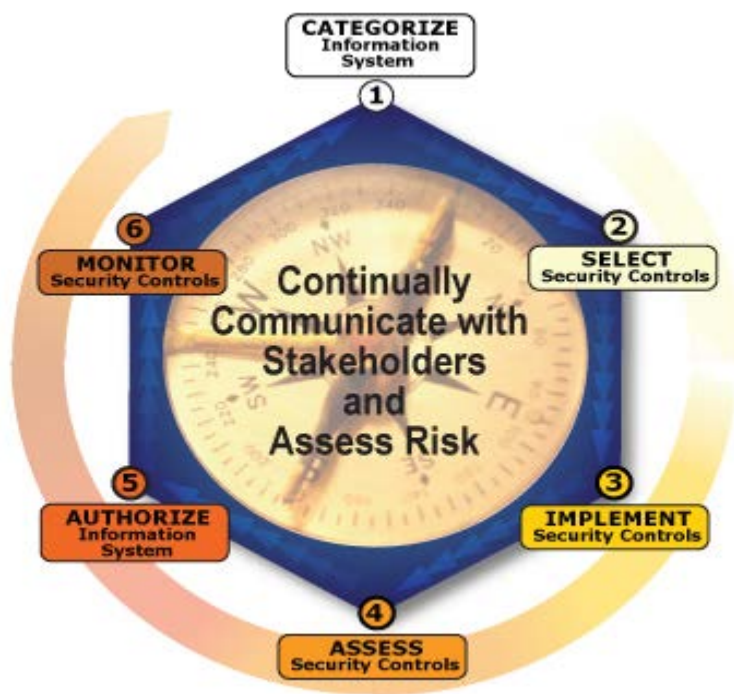
For additional information regarding the RMF, see NIST SP 800-37.

3.2 FUNDAMENTALS OF THE RMF

Organization-Wide Risk Management
Managing IS-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning and managing

projects, to individuals on the front lines developing, implementing, and operating the systems supporting the organization's core missions and business processes. Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization.

3.2.1 INFORMATION SYSTEM BOUNDARIES

Well-defined boundaries establish the scope of protection for organizational ISs (i.e., what the organization agrees to protect under its direct management control or within the scope of its responsibilities) and include the people, processes, and information technologies that are part of the systems supporting the organization's missions and business processes. IS boundaries are established in coordination with the security categorization process and before the development of the SSP. IS boundaries that are too expansive (i.e., too many system components and/or unnecessary architectural complexity) make the risk management process extremely unwieldy and complex. Boundaries that are too limited increase the number of ISs that must be separately managed and as a consequence, unnecessarily inflate the total information security costs for the organization.

Establishing IS Boundaries
Organizations have significant flexibility in determining what constitutes an IS and its associated boundary. In addition to consideration of direct management control, organizations may also consider whether the information resources being identified as an IS:

   a. Support the same mission/business objectives or functions and essentially the same operating characteristics and information security requirements.
   b. Reside in the same general operating environment (or in the case of a distributed IS, reside in various locations with similar operating environments).
   c. Reside in the same geographic area (e.g., a site).

Since commonality can change over time, the determination of the IS boundary should be revisited periodically as part of the continuous monitoring process. ISOs shall consult with key participants (e.g., AO, SCA, ISSO and other individuals with a vested interest when establishing or changing system boundaries). The process of establishing IS boundaries and the associated risk management implications is an organization-wide activity that takes into account mission and business requirements, technical considerations with respect to information security, and programmatic costs to the organization.

Once an IS boundary is set, any interconnections with systems outside of that authorization boundary that are approved by a different AO are governed by an Interconnection Security Agreement. An ISA is not required for a system authorized by DSS AO. A Network Security Plan (NSP) is required to document an interconnection between two or more separately authorized ISs by a DSS AO.

3.2.2 BOUNDARIES FOR COMPLEX INFORMATION SYSTEMS

Security architecture plays a key part in the security control selection and allocation process for a complex IS. This includes monitoring and controlling communications at key internal boundaries among subsystems and providing system-wide common controls that meet or exceed the requirements of the constituent subsystems inheriting those system-wide common controls. While subsystems within complex ISs may exist as complete systems, the subsystems are, in most cases, not treated as independent entities because they are typically interdependent and interconnected.

Security controls for the interconnection of subsystems are employed when the subsystems implement different security policies or are administered by different authorities. The extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the complex IS, can be determined by combining security control assessments at the subsystem level and adding system-level considerations addressing interface issues among subsystems. This approach facilitates a more targeted and cost-effective risk management process by scaling the level of effort of the assessment in accordance with the subsystem security categorization and allowing for reuse of assessment results at the IS level.

3.2.3 FEDERAL INFORMATION SYSTEMS

Federal ISs are owned and authorized by a federal agency under the NISP. Contractors may operate and provide local administration of the federal IS, as required and approved by the owning agency's AO.

Upon request by the GCA, the contractor will establish a government-designated space for the operation of a federal IS processing classified information in cleared contractor facilities. The contractor will ensure the government-designated space is clearly identified for DSS and the customer/GCA to prevent confusion regarding oversight responsibilities. DSS does not have physical security oversight or AO responsibility for federal IS operating in a designated government space within a cleared contractor facility.

If a government customer or GCA needs to locate a federal IS at a contractor cleared facility that lacks a government-designated space, the ISSM will coordinate with the applicable customer/GCA to request DSS concurrence to operate the federal IS in the area under DSS security cognizance if:

a. The Customer or applicable GCA maintains accountability for the federal IS and serves as the AO for that IS.
b. The federal IS directly supports a program or contract already functioning in the area under DSS security cognizance.
c. There are no connections between the federal IS and any IS authorized by DSS.
d. There is no unapproved backside connections between the Federal IS and the SECRET Internet Protocol Router Network (SIPRNET).
e. The inclusion of a federal IS in an area under DSS cognizance will not require physical security requirements beyond those established by the NISP and approved by DSS for classified processing.

4   RISK MANAGEMENT FRAMEWORK SIX STEP PROCESS

The RMF and associated RMF tasks apply to both ISSMs and CCPs. In addition to supporting the authorization of ISs, the RMF process supports maintaining the security posture of the IS, and facilitating senior leader decision making related to operational risk. Execution of the RMF tasks by common control providers, both internal and external to the organization, helps to ensure that the security capabilities provided by the common controls can be inherited by IS owners with a degree of assurance appropriate for their information protection needs. This approach recognizes the importance of security control effectiveness within ISs and the infrastructure supporting those systems.

The RMF is life cycle-based; therefore, ISSMs will need to revisit various tasks over time to manage their ISs and the environment in which those systems operate. Managing information security-related risks for an IS is viewed as part of a larger organization-wide risk management

activity carried out by senior leaders. The RMF must simultaneously provide a disciplined and structured approach to mitigating risks from the operation and use of organizational ISs and the flexibility and agility to support the core missions and business operations of the organization in a highly dynamic environment of operation.

The ISSM shall be appointed in writing and shall ensure the IS is designed, developed, and implemented with required security features and safeguards. A single appointment letter, signed by the FSO, designating the area of responsibility (e.g., Commercial and Government Entity (CAGE) code or facility) shall suffice for all IS under the ISSM's purview. The ISSM may also assign an ISSO to fulfill certain responsibilities of the RMF. These responsibilities shall be reflected in the appointment letter by the ISSM and acknowledged by the appointed ISSO. The ISSM retains overall responsibility for the security of the IS.

The ISSM/ISSO is responsible for the following tasks when categorizing the IS. ISSMs should coordinate categorization requirements with the IO, Program Manager and other stakeholders. Absent of requirements from customer, the DSS initial baseline is moderate-low-low in accordance with NISPOM Ref 8-301.

4.1 RMF STEP 1, CATEGORIZE
Step 1 of the RMF focuses on categorizing the IS. ISs shall be categorized based on the impact due to a loss of confidentiality, integrity, and availability of the information or IS.

Task 1-1: Categorize the IS and document the results in the SSP.
    a. Industry shall perform a Risk/Threat Assessment for specific concerns for their Facility/Program. (See Risk Assessment Report (RAR) template.) Risk Assessments results should be reviewed to examine the facility's threat picture and determine if tailoring controls are required. Based on the risk assessment, DSS may change the system categorization with the concurrence of the Information Owner. Cleared contractors with a high threat picture will require IO/GCA concurrence on Categorization. Follow the appropriate Security Classification Guides (SCG) for RAR results.
    b. Establish boundaries.
    c. The security categorization process is initiated by the ISSM, who proposes the initial impact levels based upon contractual requirements (i.e. DD Form 254).
    d. The ISSM categorizes the IS based on the impact due to a loss of confidentiality (moderate/high), integrity (low/moderate/high), and availability (low/moderate/high) of the information or IS according to information provided by the Information Owner or DSS.
    e. ISSM shall assign qualified personnel to RMF roles.
    f. The ISSM shall start the initial SSP to document the description, including the system/authorization boundary and personnel.

Security impact levels are defined as Low, Moderate or High for each of the three IS security objectives (Confidentiality, Integrity and Availability). For example, an IS may have a Confidentiality impact level of Moderate, an Integrity impact level of Moderate, and an Availability impact level of Low.

The impact values shall be documented in the SSP along with the research, key decisions, approvals, and supporting rationale. The following paragraphs provide guidance in defining

impact levels for all ISs under the purview of DSS in those instances the data owner requires categorization beyond the DSS baseline.

Confidentiality

The confidentiality impact level for all NISP systems will be moderate or high. The Confidentiality Impact Level is:

    a. **Moderate** if the unauthorized disclosure of any information processed, stored and transmitted by the IS could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

    b. **High** if the unauthorized disclosure of any information processed, stored and transmitted by the IS could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

Integrity

The Integrity Impact Level is:

    a. **Low** if the unauthorized modification or destruction of any information processed, stored and transmitted by the IS could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

    b. **Moderate** if the unauthorized modification or destruction of any information processed, stored and transmitted by the IS could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

    c. **High** if the unauthorized modification or destruction of any information processed, stored and transmitted by the IS could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

Availability

The Availability Impact Level is:

    a. **Low** if the disruption of access to or use of any information processed, stored and transmitted by the IS could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States. (e.g., more than 24 hours).

    b. **Moderate** if the disruption of access to or use of any information processed, stored and transmitted by the IS could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States. (e.g., less than 24 hours).

    c. **High** if the disruption of access to or use of any information processed, stored and transmitted by the IS could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States (e.g., minutes).

The following provides amplification of terms used in determining impact levels.

    a. A **limited** adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

        (1)   Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;

        (2) Result in minor damage to organizational assets;

        (3) Result in minor financial loss; or

        (4) Result in minor harm to individuals.

b. A **serious** adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

        (1) Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;

        (2) Result in significant damage to organizational assets;

        (3) Result in significant financial loss; or

        (4) Result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

c. A **severe or catastrophic** adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

        (1) Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

        (2) Result in major damage to organizational assets;

        (3) Result in major financial loss; or

        (4) Result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

4.2 INFORMATION SYSTEMS TYPES

There are many ISs types and system configurations that operate within cleared contractor facilities. However, the three predominant IS types are the Multi-User Standalone (MUSA), the Local Area Network (LAN), Interconnected System and other Wide Area Network (WAN). The information below identifies the particular types of IS seen in industry.

4.2.1 MULTI-USER STANDALONE SYSTEMS

Multi-user systems serve multiple users, but only one user at a time, and do not sanitize between users. SUSAs simply support one general user. Privileged users (systems administrators) should not be included when determining the number of users on the system. The ISSM or designee shall utilize the DSS Overlays (Appendix D) to assist with tailoring control selection.

4.2.2 LOCAL AREA NETWORK

A LAN consists of two or more connected workstations for the purpose of sharing information. The physical security parameters within SSPs vary between closed areas and various configurations of restricted areas. However, to avoid the use of removable hard drives on multiple systems, LANs that reside in a closed area are left up and running when unattended. A LAN can be as simple as two interconnected laptops through a category 5 cross-over cable in a peer-to-peer configuration and as complex as a thousand desktops connected by multiple switches and routers traversing several buildings using Active Directory to push group security policies throughout the domain. The defining characteristics of LANs, in contrast to WANs, include their much higher data transfer rates, smaller geographic range, and lack of a need for leased telecommunication lines.

4.2.3 UNIFIED NETWORKS

A unified network applies when all involved AOs concur that there will be a single security policy for the entire WAN. For WANs where all the nodes are authorized by DSS, the AO of the host node will authorize the network.

4.2.4 INTERCONNECTED NETWORKS

An interconnected network consists of two or more separately authorized systems connected together. Interconnected networks may be contractor-to-contractor or government-to-contractor connections, or a combination of both.

A WAN is a computer network that covers a broad area (e.g., any network whose communications links cross metropolitan, regional, or national boundaries), or, more formally, a network that uses routers and public communications links. This is in contrast with personal area networks (PANs), local area networks (LANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area (e.g., a city, state) respectively. The largest and most well-known example of a WAN is the Internet.

WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private; whereas, others are publicly accessible and have specific requirements for access and interconnection.

4.2.4.1   CONTRACTOR-TO-CONTRACTOR NETWORKS

Network Security Plans
A NSP must be written for any interconnection between two or more separately authorized ISs including two or more systems owned by the same ISSM at the same facility or campus (CAGE code).

The NSP is used to document the security posture of the interconnecting systems in a standalone document separate from the associated profiles for the interconnected systems. The NSP provides the AO with an overall view of the WAN and interconnections along with the associated security requirements. The NSP is assigned its own Unique Identifier (UID) and is authorized as an IS. Utilizing an NSP for a WAN enables the AO to add new connections or nodes to the system without requiring the existing nodes to be reauthorized.

The NSP is submitted and managed by the designated host ISSM. The NSP is submitted into the process like standard SSPs. The host ISSM and responsible DSS office are responsible for authorizing the interconnected network's NSP.

NSP Content
The responsibility for creating, gaining authorization, and maintaining an NSP belongs to the ISSM responsible for the "host" node. If the WAN is authorized by DSS, the authorization document for the WAN will be referred to as the NSP. If the WAN is not authorized by DSS, the name and content of this document may be different from a standard DSS NSP. This is typically encountered when a DSS-authorized IS is connecting to a WAN authorized by another government entity or AO. This type of connection also requires an MOU/ISA or an MOA signed by all AOs with systems connected.

At a minimum, an NSP should include the following information for the WAN:

a. AO Unique identification (ID) and IS name.
b. Physical addresses for connected sites.
c. Point of contact (POC) information for each site.
d. Highest classification of data with any requirements identified.
e. Minimum clearance level required for user access to the WAN.
f. Description of the system along with a diagram showing all connections.
g. Encryption method and devices in use.
h. Security responsibilities for the WAN and nodes.
i. Network connection rules including a statement from the ISSM as to whether or not full node authorization will be required for connection or if an interim approval is sufficient.
j. Signed and dated statement from the ISSM attesting that there are no additional connections to the WAN not identified in the NSP.
k. A network participation data sheet for each node which includes requirements listed in bullets a-h above and a description of the node system. This must be signed by the node ISSM.
l. For any node not authorized by DSS an authorization letter or a signed MOU/ISA/MOA. If the node is under a DSS-authorized MSSP, the profile associated with the node must be identified.
m. NISPOM Chapter 8 compliant security policies and procedures for any systems or components seeking authorization as part of the NSP.
n. Controlled Interfaces (Firewall) description with ports and protocols.
o. Access control lists (if applicable).
p. Intrusion Detection System (IDS) requirements (if any).
q. For auditing purposes, record activities occurring across the interconnection.
r. Identify any Identification and Authentication (I&A) methods used to authenticate users across the interconnection.
s. Specific virus scanning or anti-virus requirements (if any).
t. Identify physical security requirements (e.g., closed or restricted area).

Under these circumstances, the NSP should also contain the following WAN connection rules:
a. All personnel will be briefed on the use of the WAN and will be knowledgeable of the NSP security requirements.
b. WAN configuration changes must be approved by the ISSM to determine if the reconfiguration constitutes a security relevant change which requires approval or reauthorization by the AO.
c. Any configuration changes affecting the node's a categorization, and/or clearance level of users must be approved by the AO for both the node and the WAN before the change can be made.
d. Other WAN connection rules could be added at the discretion of the ISSM and/or AO.

4.2.5 SUBMITTING THE NSP TO DSS FOR AUTHORIZATION
The Network/Host ISSM/ISSO will submit the NSP and include copies of current authorization letters for all nodes connected to the WAN. The DSS reviewer will verify all nodes have a current authorization letter in the NSP package. In addition, a signed copy of each node ISSM's participant data sheet will be included with the NSP submitted to DSS for review and authorization. When the NSP is subsequently submitted for reauthorization (e.g., when adding a new node) the Network ISSO/ISSM will include current authorization letters for all nodes submitted. If the NSP is submitted with copies of expired authorization letters, review and authorization will be delayed until updated copies are obtained.

NSPs covering two or more separately authorized systems at the same facility, campus or CAGE and managed by the same ISSM can be simplified. In such cases, the ISSM can submit a single page NSP that address requirements 1-7, 10 and 13 above and includes each nodes' AO UID (and IS profile if under a MSSP), protection level, location, if different from facility address, classification of data processed with any additional caveats, minimum clearance of users and node name.

    a. The need for interconnection or WAN establishment is noted by two or more ISs to support contractually related work or programs.

    b. One ISSM is designated "host" node and assumes role of "Network ISSO" for the WAN or interconnected system.

    c. Host node ISSM or "Network ISSO" prepares the NSP.

        (1) Collects signed participant data sheets and local authorization letters from all node ISSMs.

        (2) Provide e-mail addresses in the package for all node ISSMs.

        (3) Ensures encryption devices are in place at all nodes. Some nodes may need to get reauthorized locally when adding the encryptor and WAN connection to the profile

        (4) Determines if an MOU/ISA is needed. If yes, uses the DSS template to create an MOU/ISA customized for the requirements. Obtains and inserts AO signature blocks onto the MOU/ISA form.

        (5) Completes the NSP document and diagram, etc. Attaches MOU/ISA (if required), authorization letters and signed participant data sheets for each node.

        (6) Assigns an AO Unique Identifier to the NSP.

        (7) Documents any devices or components that are to be authorized with the NSP instead of in an associated profile. This is rare, but all NISPOM required information is required. Typically, an SSP attachment to the NSP may be used.

        (8) Ensures completed package is submitted to the AO via OBMS.

    d. The ISSP will review the NSP for completeness and make certain all required documentation is included.

        (1) If the NSP includes components/devices not authorized under an associated profile (rare), the ISSP will schedule a visit to validate these components.

        (2) There may be cases where an NSP is granted an Interim Approval to Operate (IATO), but typically, an NSP is issued an Approval to Operate (ATO) when all documentation is correct.

        (3) Any required MOU/ISAs based on node connections documented in the NSP must be signed by all AOs before the NSP is approved.

    e. AO will sign and distribute the NSP's ATO. The NSP ATO will be sent back to the Network ISSO and responsible DSS personnel.

    f. Network ISSO provides each node with a copy of the NSP, its authorization letter, and any associated MOU/ISAs.

Connecting to a WAN Authorized by DSS

The NSP for a DSS-authorized WAN is processed in the same manner as an SSP. The Network ISSO is responsible for creating and submitting the NSP through the review process for authorization by the host AO.

Realizing that adding nodes to a WAN could potentially change the security posture of the WAN, each node to be added must be evaluated for clearance and need-to-know concerns. When DSS is the WAN AO a connection determination must be made. In order to provide consistency, the following rules will be applied. The final node connection determination is still subject to the discretion of the AO.

Adding a node to an existing DSS WAN – Step-by-Step

Step 1:
Host node ISSM or "Network ISSO":
  a. Updates the NSP.
  b. Collects signed participant data sheets and local authorization letters from the new node ISSM(s).
  c. Verifies all existing nodes' participant data is current and requests updated information as needed.
  d. Provides e-mail addresses for all node ISSMs.
  e. Ensures encryption devices are in place at new nodes. NOTE: Some nodes may need to be reauthorized locally when adding the encryptor and WAN connection to the profile.
  f. Determines if an MOU/ISA is needed for the new nodes' connection. If yes, uses the DSS template to create an MOU/ISA customized for the requirements.
  g. Obtains and inserts AO signature blocks onto the MOU/ISA form.
  h. Updates the NSP document and diagram, etc.
  i. Attaches MOU/ISA (if required), local authorization letters for new node(s) and any updated local authorization letters or signed participant data sheets.
  j. E-mails the completed package to DSS AO and carbon-copies DSS personnel as required by the process manual.

Step 2:
The ISSP will review the NSP for completeness and ensure all required documentation is included. If the NSP includes components/devices not authorized under an associated profile (rare), the ISSP will schedule a visit to validate these components if there were changes (rare). Required MOU/ISAs must be signed by all AOs before the node is allowed to connect to the WAN.

Step 3:
The ISSP will forward the updated draft ATO for the NSP to the AO. AO will sign and send the signed ATO for the NSP back to the Network ISSO. The Network ISSO will update all nodes with a copy of the ATO and updated NSP along with any new or modified MOU/ISAs.

Connecting to a WAN not authorized by DSS
When a DSS-authorized node is connecting to a non-DSS authorized WAN, the approval to connect is granted by the non-DSS AO. An MOA or MOU/ISA is required to document security responsibilities for the connection. The MOA/MOU/ISA's content should be limited to ISs security/AO responsibilities only and not include other information such as funding requirements. DSS has a standard MOU/ISA/MOA template that should be used. The MOU/ISA or MOA should state whether a full ATO is required before a DSS controlled contractor node can be connected to the WAN and provide POC information. The MOU/ISA/MOA must require all nodes and the WAN be authorized in accordance with the respective certification and authorization requirements documents.

The contractor can write an SSP for the node under DSS cognizance provided that it is not explicitly denied in the MOU/ISA/MOA. The addition of a like system to the contractor node under a DSS approved MSSP must be approved by the WAN AO or designated WAN point of contact. The contractor must contact the WAN POC to seek permission to add the like system prior to the addition unless otherwise directed by the WAN AO. The decision of the WAN POC

must be communicated to the IS Rep, ISSP and Field Office Chief for the contractor node. If the WAN POC or AO determines that like systems can be added to the DSS approved MSSP for the node without seeking further approval of the WAN Cognizant Security Agency (CSA), the contractor is still required to notify their assigned ISSP.

4.2.5.1 GOVERNMENT-TO-CONTRACTOR NETWORKS

4.2.5.1.1 GOVERNMENT INTERCONNECTION AGREEMENTS

For the purposes of this manual, MOU/ISAs, MOAs and Interconnection Security Agreements are used interchangeably. The term MOU/ISA/ISA may be used generically throughout this document in reference to all three types of agreements. MOU/ISAs created for other purposes (e.g., sharing a space or closed area) are not addressed in this manual.

An MOU/ISA/ISA between DSS and the GCA is required for all government to contractor connections to include connections over National Security Agency (NSA)-approved encryption.

An MOU/ISA is not required for contractor-to-contractor connections if DSS is the AO for both authorized ISs, only an NSP is required for such connections. If the contractor requires an MOU/ISA, that is between the two contractors who require the connection. The purpose of an MOU/ISA is to adjudicate the differences in requirements of different AOs and to establish roles and responsibilities. Many GCAs and program offices have standard MOU/ISA formats that are routinely utilized for all MOU/ISAs. The GCA may use their format if they'd like; however, DSS may levy additional requirements in order to be NISPOM compliant.

Interconnected systems that result in the requirement for an MOU/ISA may range from complex WANs to simple connections between two standalone systems.

All MOU/ISAs must be sent to NAO for coordination and signature. AO requires a minimum of 30 days to coordinate and properly staff all MOU/ISAs for signature. MOU/ISAs are valid for a maximum of three years, at which time they must be resubmitted for both GCA and DSS review, and signature. They may be rescinded by either party (DSS or GCA) with prior notification to, DSS or the GCA, at any time.

4.2.6 MOU/ISA/ISA CONTENT

If an MOU/ISA is submitted in a format other than the DSS approved format, more DSS internal reviews are required prior to approval. Processing and approval time within DSS will be impacted greatly. It is recommended that the DSS approved MOU/ISA format be used.

All MOU/ISA/ISAs must contain the following minimum information:
a. Date MOU/ISA.
b. Names and signatures of AO.
c. Name of Network ISSM/ISSO and responsibilities.
d. High-level description of and usage of the network.
e. Contract or program name.
f. Name and location of facilities involved.
g. Security points of contact and phone numbers.
h. Names, numbers or system identifiers for systems involved.
i. Highest classification of data.
j. MOU/ISA expiration date or review frequency (if applicable).
k. Categorization (CIA Impact Level).

l. Minimum clearance level required of users.
m. Network type: Unified or Interconnected (usually interconnected).
n. Documentation of any existing connections to DISN circuits.
o. A statement that there is no further connection to any DISN network not outlined in the MOU/ISA and none will be added in the future (Secure Internet Protocol Router Network (SIPRNet), SDREN, DISN-LES, etc.).
p. Encryption method.
q. A statement regarding required authorization status for interconnected sites and informing Network ISSO about any changes in authorization status.
r. A start and end date.
s. MOU/ISA valid for a maximum of up to three years.
t. A requirement to be signed by all parties before the MOU/ISA is effective.

MOU/ISA Changes and Invalidations
MOU/ISAs are valid for three years or until system changes occur that affect the security posture and agreement defined in the MOU/ISA. Some MOU/ISAs specify a pre-determined review frequency. During the review, security parameters, the need for the MOU/ISA, POC information and AO signatory information should be verified. If changes are required, a new MOU/ISA should be vetted and routed for signatures.

MOU/ISAs may become invalid if the security posture of a node or the WAN itself changes. Changes must be evaluated by the signing AOs to determine the impact (if any) on the authorization of the WAN and/or the validity of the MOU/ISA.

Changes that may affect the security posture of the WAN or a node should be approved by the AOs prior to implementation.

4.2.6.1 INTERNATIONAL INTERCONNECTIONS/SECURE COMMUNICATIONS PLAN (SCP)

Requests to establish international secure communications links between U.S. cleared contractors and foreign governments or foreign cleared contractors require additional supporting artifacts. When submitting the SSP within OBMS, the ISSM shall select "International" as a special category for the IS/UID. The SSP format can be used to support the official SCP for approval. If separate SCP is approved by the Designated Security Authorities (DSAs) or as part of a Program Security Instruction (PSI), the SCP shall become an attachment to the SSP. Industry shall include the following as supporting documentation with the SSP:
a. Export Authorization.
b. Export Procedures.
c. Program Security Instruction (if applicable).

Specific Requirements
The following security requirements must be met for each communication node for the transmission of classified information:
a. The Facility Security Officer/ISSM shall appoint a cleared company employee as the designated representative of the communication node. The designated representative may be the ISSM, ISSO or another designee.
b. The FSO shall appoint one or more Releasing Officers (RO) and Designated System Operators (DSO) for the communication node that will be appropriately trained. The ROs and DSOs must possess a security clearance at least to the highest classification level of the accessible classified information, and be a contractor employee and citizen of the

nation in which the communication node is located. The RO will be designated in writing as an empowered official to act on behalf of their respective companies. Each RO will have the authority to ensure into any aspect of a proposed export or temporary import and verify the legality of the transaction and the accuracy of the information to be transferred. The RO may refuse to sign any request for release without prejudice or other adverse recourse.

c. The ISR will brief the FSOs, who will in turn brief the relevant staff, RO, and DSO on what information and technology is releasable under the contract. The employees shall acknowledge the briefing in writing. The boundaries of what information is releasable will be carefully defined, particularly in cases where associated technology or information is not releasable. The briefing record will include the date, the identity of the persons conducting and receiving the briefing, and specific acknowledgment by the person being briefed that they:

   (1) Understand the extent of the information and technology approved for release;
   (2) Are familiar with the security procedures and record keeping requirements pertinent to these transmissions;
   (3) Are aware of the criminal penalties that attach to violations of the export statutes; and
   (4) Have been given a Government POC who can clarify the nature and extent of the material that may be released or the applicable security procedures.

d. Only DSOs will be authorized to place and receive calls and/or to operate equipment. The DSO will be thoroughly familiar with the technical data to be transferred, the project related technology export licenses, and the specific description of material that is authorized for disclosure. The DSO will be responsible for notifying the FSO/ISSM of any required maintenance or repair to the net hardware.

e. The ISSM or designee and the DSOs will be responsible for the secure operation of the communication node in accordance with these instructions and Local Operating Procedures (LOPs).

f. The FSO or ISSM for the system will prepare LOPs for the communication node for AO as an attachment to the SSP.

g. Authority to Communicate. Authority to activate the secure dedicated communications link will be granted by the AO after concurrences are received from the Designated Security Authorities (DSAs) from the United States and Foreign Government.

4.2.7 SPECIAL CATEGORIES

Special category systems, as described in the NISPOM, will follow the same authorization process as all other information systems; however, it is expected they will implement a tailored set of security controls and make use of compensating controls (when necessary) to provide the acceptable level of protection. Specific application of security measures to protect the system and the data residing on them will be addressed in the SSP.

The contractor will select and implement the appropriate baseline of security controls and, when necessary, apply compensating controls to provide adequate security of the IS. The ISSM will provide the AO with complete rationale and justification for how the compensating controls provide an equivalent security capability or level of protection for the ISs.

4.2.7.1   COPIERS

Multifunction copiers combine a PC, printer, and scanner into one container. These devices typically have non-volatile memory, hard drives, an operating system, and networking capability. Some utilize Radio Frequency (RF) Identification (RFID) technology for device inventory or status management. Copiers with these features are to be authorized as a system. Separate

authorization is only required for standalone devices. Separate authorization is not required for these devices when connected to an IS as a peripheral device. In these instances, the multifunction device should be included in the connected system's authorization plan. In particular, area upgrade and monitoring may be necessary to ensure physical security. (NISPOM Chapter 5, Section 6 (Reproduction)) is applicable to these systems. Copiers that do not have non-volatile memory or hard drives do not require authorization to process classified information.

4.2.8 TYPES OF SECURITY PLANS
Plans submitted to DSS must be submitted using the applicable DSS-provided system security plan templates in order to accommodate timely reviews. The templates can be requested from the DSS web site. Once completed, plans should be kept from public disclosure, as they can provide adversaries insight to how classified information is being protected.

There are three types of plans that can be submitted to the AO:
   a. System Security Plan;
   b. Master Systems Security Plan; and
   c. Network System Plan.

One system security plan may include IS that are being authorized to support multiple program areas as long as the users have the proper authorization and need-to-know for all information on the system. It is recommended that data from different programs remain separated to facilitate potential removal of data at the end of contract.

4.2.8.1 SYSTEM SECURITY PLAN
The SSP is the document used to identify the Categorization and Selection of Controls for protection measures to safeguard classified information being processed. The process flow for submitting SSPs is explained in the OBMS job aids.

4.2.8.2 MASTER SYSTEMS SECURITY PLAN/TYPE AUTHORIZATION
NISP SP 800-37 defines Type Authorization as "A type authorization is an official authorization decision to employ identical copies of an information system or subsystem (including hardware, software, firmware, and/or applications) in specified environments of operation. This form of authorization allows a single authorization package (i.e., security plan, security assessment report, and plan of action and milestones) to be developed for an archetype (common) version of an information system that is deployed to single location (Cage Code and ISSM), along with a set of installation and configuration requirements or operational security needs, that will be assumed by the hosting organization at a specific location. The type authorization is used in conjunction with the authorization of site-specific controls (e.g., physical and environmental protection controls, personnel security controls) inherited by the information system." The term "Master" indicates the intent to have like systems authorized under one Type Authorization package.

DSS "Authorization" is required for the Type Authorization request, before the system is allowed to process classified data.

Within OBMS, the ISSM must submit request for a Type Authorized system within using the "Self-Certification" link.

4.2.8.2.1 MSSP GENERAL REQUIREMENTS

An MSSP must be specific to the operating environment. For example, a separate plan must be prepared for restricted areas and closed areas. An MSSP must also reflect operating systems approved for Type Authorization. No variances are allowed.

Examples of MSSP types	
SUSA in restricted area	Interconnected System in a restricted area/PDS
SUSA in closed area	Interconnected System in a closed area/PDS
Windows 10 MUSA in a restricted area	Interconnected System in a restricted area
MUSA in a closed area	Interconnected System in a closed area
LAN in a restricted area/Protected Distributed System (PDS)	
LAN in a closed area/PDS	The ISSM is only allowed to add additional workstation(s) under a MSSP for Interconnected Systems.
LAN in a restricted area	
LAN in a closed area	

4.3 RMF STEP 2, SELECT

Step 2 of the RMF focuses on selecting the security controls applicable to the IS. The ISSM, along with assistance from the ISSO (if applicable) is responsible for the following tasks:

    a. **Task 2-1:** Identify and document the baseline security controls applicable to the IS, based upon the Confidentiality, Integrity and Availability impact levels determined during RMF Step 1. This is accomplished using the tables located in Appendix C of this document and, if desired, exercising the option to implement a DSS approved Overlays to a baseline. Security controls are identified as System Specific (S), Common (C) or Hybrid (H). (The abbreviations are generally used in charts only.) System-specific security controls are security controls specific to an IS and are the responsibility of the ISSM. Common controls are security controls that are inheritable by one or more organizational ISs and are typically provided by the organization or the infrastructure. Hybrid security controls are security controls that are implemented in an IS in part as a Common control and in part as a System Specific control and must be taken into consideration by the ISSM. Security controls shall be documented in the SSP.

    b. **Task 2-2:** Tailor the controls as needed, i.e. tailor in controls to supplement the set of selected controls, tailor out or modify the controls, as applicable. If a security control identified in the baseline set of controls is tailored out, justification must be provided in the SSP template, describing the rationale as to why the control does not apply or how it is satisfied by other mitigating factors. At the discretion of the AO, a Risk Acknowledgement Letter (RAL) may be required from the GCA as a supporting artifact for controls tailored out based on Program or system requirements. Security controls may also be added (i.e., tailored in) as necessary depending upon the information system and/or its environment of operation.

Common Controls:

- **Support multiple ISs efficiently and effectively as a common capability;**
- **Promote more cost-effective and consistent security across the organization and can also simplify risk management activities; and**
- **Significantly reduce the number of discrete security controls that have to be documented and tested at the IS level which in turn eliminates redundancy, gains resource efficiencies, and promotes reciprocity.**

CNSSI 1253 identifies security controls in the baseline that may be implemented as common controls. These suggestions are intended to provide guidance to assist with implementation planning. The final determination of which security controls will be implemented as common controls will vary depending on the system and its intended environment/deployment.

    c. **Task 2-3:** Develop a strategy for continuous monitoring of the security control effectiveness. This information may be included within the SSP and a separate document is not required. This information is used to determine whether the planned security implementation is acceptable in accordance with the RMF. Ongoing monitoring of the security controls is a critical part of risk management that must be developed early, and throughout the system development. Effective monitoring includes configuration management and control, security impact analyses on proposed changes, assessment of selected security controls, and security status reporting.

    d. **Task 2-4:** Review and approve the SSP. The ISSM will submit the initial SSP to DSS for concurrence with the categorization decision and security controls selection. Any tailoring out or modification to the baseline controls and overlay controls have SCA concurrence prior to implementation. Supporting artifacts for this step include the initial SSP with categorization and security control selection justifications, any mitigation strategies, and the Risk Assessment Report (RAR). To pass OBMS validation, The ISSM or designee will need to upload a blank Certification Statement and add the Profile extension for the RAR. Review the OBMS Job Aids for using the application at http://www.dss.mil/diss/obms.html.

4.4 RMF STEP 3, IMPLEMENT

Step 3 of the RMF focuses on implementing the security controls selected for the IS (i.e., developing or building the IS). The ISSM, with assistance from the ISSO, is responsible for the following tasks:

    a. **Task 3-1:** Implementing the security controls specified in the SSP, as reviewed by the ISSP. The ISSM may conduct initial security control assessment during this step to facilitate early identification of weaknesses and deficiencies.

    b. **Task 3-2:** Documenting the security control implementation in the SSP providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs). The documentation shall include any additional information necessary to describe how the security capability required by the security control is achieved at the level of detail sufficient to support control assessment. Initial control assessment procedures and assessment results may also be included to support additional RMF steps and avoid repetitive assessment activities.

4.5 RMF STEP 4, ASSESS

Step 4 of the RMF focuses on assessing the security controls applicable to the IS and includes the following tasks:

    a.Part 1-Industry

    (1) **Task 4-1:** The ISSM will conduct an assessment of the security controls in accordance with the security procedures defined in the SSP to ensure the security controls are implemented correctly, operating as intended, and meet the security requirements for the IS. The ISSM may use the Security Content Automation Protocol (SCAP), DISA's Security Technical Implementation Guidelines (STIGs) Viewer and the DSS Technical

Assessment job aids to support the initial Assessment. The ISSM is allowed to use other tools.

(2) **Task 4-2:** The ISSM shall update the SSP to reflect the actual state of the security controls, as required, based on the vulnerabilities of the security control assessment, reassessment, and completion of any remediation actions taken. The ISSM will submit the SSP, Certification Statement, RAR and POA&M to DSS for review and authorization consideration via OBMS. Review applicable Security Classification Guidance and ensure only unclassified attachment are uploaded within OBMS. When supporting artifact is deemed classified, please contact assigned ISSP for guidance.

Submission Artifacts	OBMS Document Types
SSP	SSP *
Certification Statement	Certification Statement*
Risk Assessment Report	Profile *
POA&M	Other
Supporting Contractual Requirement (DD254, Request for Proposals etc.)	Other
Other SSP artifacts (i.e. Standard Operating Procedures (SOPs), RALs, ISA/MOU)	Other

*Required artifacts for OBMS validation

4.6 RMF STEP 5, AUTHORIZE
Step 5 of the RMF focuses on formally authorizing the IS for operation.

(**DSS Internal Process.)**
   a. **Task 5-1:** The SCA/ISSP receives the Security Authorization Package, performs SSP review and conducts an on-site validation/assessment. Any issues/vulnerabilities/ weaknesses identified during assessments of any kind will be documented on a POA&M, outline the severity of the vulnerability, plan to mitigate with timelines.
   b. **Task 5-2:** The SCA/ISSP assesses the information provided in the security authorization package regarding the current security state of the system to determine the risk to organizational operations, organizational assets, individuals, other organizations, or national security. RAR may be employed to provide additional information on threats, vulnerabilities, and potential impacts as well as the analyses for the risk mitigation recommendations.
   c. **Task 5-3:** The explicit acceptance of risk is the responsibility of the AO. The AO will consider many factors to determine if the risk to classified information, the IS, individuals, other organizations, or national security is acceptable. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision. The AO will issue an authorization decision for the IS and the common controls inherited by the system after reviewing all of the relevant information and, where appropriate, consulting with other organizational officials.

The authorization decision document (i.e., Authorization to Operate and Denial of Authorization to Operate (DATO)) conveys the security authorization decision from the AO to the ISSM, and other organizational officials, as appropriate. The authorization decision document contains the following information:
   a. Authorization decision.
   b. Terms and conditions for the authorization.

      c.   Authorization duration.
(1) Time driven – AO may identify an expiration date, not to exceed three years.

4.7 RMF STEP 6, MONITOR

An effective organizational information security program includes a continuous monitoring program integrated into the system development life cycle to determine if the set of deployed security controls continue to be effective over time in light of the inevitable changes that occur. Continuous monitoring activities support the concept of near real-time risk management through ongoing security assessment and risk analysis, and recording results in system documentation (e.g., SSPs, SARs, and POA&Ms).

An effective continuous monitoring program includes:
    a. Configuration management and control processes for ISs;
    b. Security impact analyses on proposed or actual changes to ISs and environments of operation;
    c. Assessment of selected security controls (including system-specific, hybrid, and common controls) based on the defined continuous monitoring strategy;
    d. Security status reporting to appropriate officials; and
    e. Active involvement by authorizing officials in the ongoing management of IS-related security risks.

The AO uses the revised and updated SAR to determine if a reauthorization action is necessary. Most routine changes to an IS or its environment of operation can be handled by the organization's continuous monitoring program, thus supporting near real-time risk management. Conducting security impact analyses is part of an ongoing assessment of risk.
    a. **Task 6-1:** The ISSM/ISSO, as appropriate, shall assess a selected subset of the security controls employed within and inherited by ISs in accordance with the organization's continuous monitoring strategy. The selection of appropriate security controls to monitor and the frequency of monitoring are based on the monitoring strategy developed by the ISSM and approved by the AO. To satisfy this requirement, organizations can draw upon the assessment results from any of the following sources, including but not limited to:
        (1) Security control assessments conducted as part of an IS authorization, ongoing authorization, or reauthorization.
        (2) Continuous monitoring activities.
        (3) Testing and evaluation of the IS as part of the system development life cycle process or audit.

The results of continuous monitoring activities shall be reported to the ISSP on an ongoing basis in the form of status reports.
    a. **Task 6-2:** The ISSM shall conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M.
    b. **Task 6-3**: The ISSM shall ensure the IS security documentation (SSP and POA&M) is updated and maintained based on the results of continuous monitoring. The updated SSP shall reflect any modifications to security controls based on risk mitigation activities carried out by the ISSM/ISSO. Continuous monitoring status reports shall reflect additional assessment activities carried out to determine security control effectiveness based on modifications to the SSP and deployed controls. The updated POA&M shall report progress made on the current outstanding items listed in the plan, address vulnerabilities assessed during the security impact analysis or security control monitoring, and describe how the ISSM intends to address those vulnerabilities. The

information provided by these critical updates helps to raise awareness of the current security state of the IS (and the common controls inherited by the system) thereby supporting the process of ongoing authorization and near real-time risk management. When updating critical information in SSPs and POA&Ms, organizations shall ensure that the original information needed for oversight, management, and auditing purposes is not modified or destroyed.

c. **Task 6-4:** The ISSM shall report the security status of the IS (including the effectiveness of security controls employed within and inherited by the system) to the ISSP and other appropriate organization officials on an ongoing basis in accordance with the monitoring strategy. Security status reporting can be event driven, time driven or both. The goal is ongoing communication with DSS to convey the current security state of the IS and its environment of operation. Security status reports shall be appropriately marked, protected, and handled in accordance with federal and organizational policies.

d. **Task 6-5:** The ISSP shall review the reported security status of IS under his/her purview (including the effectiveness of security controls employed within and inherited by the systems) on an ongoing basis in accordance with the continuous monitoring strategy. This review shall determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or national security remains acceptable.

e. **Task 6-6:** The ISSM shall implement an IS decommissioning strategy, which executes required actions when a system is removed from service. Organizations shall ensure that all security controls addressing IS removal and decommissioning (e.g., media sanitization, configuration management and control) are implemented. Organizational tracking and management systems (including inventory systems) shall be updated to indicate the specific IS components being removed from service. Users and application owners hosted on decommissioned IS shall be notified as appropriate, and any security control inheritance relationships shall be reviewed and assessed for impact.

The AO shall formally decommission the IS by issuing an IS removal and Decommissioning letter.

4.8 FAMILY: ACCESS CONTROL

4.8.1 AC-1   ACCESS CONTROL POLICY AND PROCEDURES
Control: The organization:
   a. Develops, documents, and disseminates to all authorized responsible personnel as required:
      (1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
      (2) Procedures to facilitate the implementation of the access control policy and associated access controls; and
   b. Reviews and updates the current:
      (1) Access control policy annually or as policy and procedures dictate changes are required;
      (2) Access control procedures annually or as policy and procedures dictate changes are required.

Supplemental 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. Related control: Program Management (PM)-9.

Control Enhancements: None.
References: NIST Special Publications 800-12, 800-100.
4.8.2 AC-2 ACCOUNT MANAGEMENT
Control: The organization manages information system accounts and:
   a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: as defined by ISSM;
   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 ISSM/ISSO or designee for requests to create information system accounts;
   f. Creates, enables, modifies, disables, and removes information system accounts;
   g. Monitors the use of information system accounts;
   h. Notifies account managers:
      (1) When accounts are no longer required;
      (2) When information system 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 at least annually, if not otherwise defined in organizational policy; and

    k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Organizations are responsible for managing information system accounts to include identifying account types and procedures for creating, activating, modifying, monitoring, disabling, and removing accounts. Definitions for types of accounts can be found in DAAPM AC-2. All accounts must be reviewed at least annually for changes in such items as staff position, office symbol, contact information, transfer, etc. [AC-2.j] the validation process shall be documented.

Supplemental 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., timezone 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:
    a. When shared/group, emergency, or temporary accounts are no longer required; or
    b. When individuals are transferred or terminated.

Some types of information system accounts may require specialized training.

Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, Maintenance (MA)-3, MA-4, MA-5, Planning (PL)-4, System and Communications Protection (SC)-13.

System/Service Accounts

System accounts are internal accounts that are used by the operating system and by services that run under the control of the operating system. There are many services and processes within the operating system that need the capability to log on internally utilizing a service account.

System/service accounts shall not be added to any general user groups and shall not have general user rights assigned to them.

Temporary/Emergency Accounts

Temporary and emergency accounts are accounts that are established for individuals not previously identified in the information system, such as inspectors, assessment team members, vendor personnel or consultants, who may require access to the system, for example, to conduct assessment, maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, organizations may establish temporary or emergency accounts for these individuals. The ISO or designee must approve the creation of temporary or emergency accounts. Temporary and emergency accounts may be for one-time use or for a very limited time period. The ISSM/ISSO/SA must be notified when temporary or emergency accounts are no longer needed, see [AC-2(2)]. See PL-4 for Rules of Behavior for users.

General User Accounts

A general user account is provided to an individual who can receive information from, input information to, or modify information on a system.

Privileged User Accounts

A privileged user account is provided to an individual who is authorized to perform security-relevant functions, such as system control, monitoring, data transfer, or administration functions that general users are not authorized to perform.

Account Creation

The ISO or designee identifies the individual(s) authorized to assign the user account identifier and authenticator(s) to system users. The supervisor must ensure all individual access requests are valid and access is work/mission-related.

Prior to granting access to any information system, the individual responsible for account creation and/or changes to access permissions shall verify that the user to whom access is being granted is appropriately cleared and indoctrinated to all levels of information that will be accessible, and that the user is in compliance with personnel security requirements. This verification shall be done via the local Security or Program Manager (PM) as applicable. In addition, the ISSM/ISSO or SA responsible for account creation shall ensure that only accesses and privileges validated by the requestor's supervisor are granted, [AC-2.c] [AC-2.d] [AC-2.i]. See also Identifier Management [IA-4] and Authenticator Management [IA-5].

User Account Disabling/Deletion [AC-2.f]

All user accounts must be disabled, generally within 24 hours, when information system users are terminated, transferred, or no longer require access to the information resource in the performance of their assigned duties. When a user's security clearance is revoked due to an incident or violation, the user's account must be disabled immediately. Disabled accounts shall be maintained for a minimum of 12 months or one review cycle, whichever is longer. Organizations must ensure that information deemed to be of value is retained before a user's account is deleted.

Group Accounts [AC-2.k; AC-2(9); AC-2(10)]

In general, group accounts are prohibited. The use of group accounts/authenticators precludes the association of a particular act with the individual who initiated that act, i.e., individual accountability. Situations should be avoided in which the group account/authenticator is effectively the sole access control mechanism for the system.

However, use of group accounts/authenticators for broader access after the use of a unique authenticator for initial identification and authentication carries much less risk. The use of group accounts/authenticators shall be explicitly authorized by the AO or designated representative.

Exceptions to this policy may include the use of group accounts in tactical/deployed environments. Use of group accounts in a tactical/watch standing environment allows rapid interchange between users whose primary focus is quick access to the system without interruption of functions or capabilities. This also avoids the potential for errors on startup as the system is shut down and restarted for a different user to logon. A list shall be used for watch stander rotations or battle station assignments, which must be retained and used to augment activity logs to correlate user identities to actions as recorded on audit logs. An alternative involves the development of a simple pop-up "change USERID" Graphical User Interface (GUI) which does not cause the system to shut down or change operations. This alternative simply changes accountability via the new user identification (USERID)/password for continuing processes under another individual member of a common functional group. Reference IA-2 and IA-2(5).

Control Enhancements:

4.8.2.1   AC-2(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

Control: The organization employs automated mechanisms to support the management of information system accounts**.**

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 to monitor account usage or to report atypical account usage. When automated mechanisms cannot be used, a manual process must be established and documented and will require explicit AO approval.

4.8.2.2   AC-2(2) ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS

Control: The information system automatically **disables** temporary and emergency accounts after **not more than 72 hours**.

Supplemental 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.

4.8.2.3   AC-2(3) ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS

Control: All password-accessible accounts must be disabled when information system users are terminated, transferred, or no longer require access to the information resource in the performance of their assigned duties. The information system automatically disables inactive accounts after **a maximum of 90 days of inactivity**. Accounts where the user has lost their security clearance will be disabled immediately.

4.8.2.4　AC-2(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

Control: The information system automatically audits account creation, modification, enabling, disabling, and termination actions and notifies, as required, appropriate individuals. This control supports insider threat mitigation. Supplemental Guidance: none. Related controls: AU-2, AU-12.

4.8.2.5　AC-2(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

Control: The organization requires that users log out when user's work day has ended or there is an extended absence (more than six hours). This control supports insider threat mitigation. Supplemental Guidance: none. Related control: SC-23.

4.8.2.6　AC-2(7) ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES

Control: 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. Disables (or revokes) privileged user accounts when privileged role assignments are no longer appropriate. This control supports insider threat mitigation. **Privileged roles** also include the auditor and data transfer agent (DTA).

Supplemental Guidance: 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.

Organizations shall establish and administer privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and tracks and monitors privileged role assignments. [AC-2(7)(a)], [AC-2(7)(b)] Privileged roles also include auditor and data transfer agent.

4.8.2.7　AC-2(9) ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS

Control: The organization only permits the use of shared/group accounts that **are operationally essential and when explicitly authorized by the AO**. This control supports insider threat mitigation.

4.8.2.8　AC-2(10) ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION

Control: The information system terminates shared/group account credentials when a member/members leave the group. This control supports insider threat mitigation.

4.8.2.9　AC-2(12) ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE

Control: The organization:
  a. Monitors information system accounts atypical usage **based on Program-unique requirements;** and

b.   Reports atypical usage of information system accounts to **the ISSM immediately upon detection**. This control supports insider threat mitigation.

Supplemental Guidance: Atypical usage includes accessing the IT at times of the day or from locations that are inconsistent with normal usage patterns in the Program. Related control: Certificate Authority (CA)-7.

4.8.2.10 AC-2(13) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

Control: The organization:

a. The organization disables accounts of users posing a significant risk **immediately or as soon as possible after discovery**. See also AU-6. This control supports insider threat mitigation.

Supplemental Guidance: Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Close coordination between authorizing officials, information system administrators, and human resource managers is essential in order for timely execution of this control enhancement. Related control: Personnel Security (PS)-4. See also AU-6. References: None.

4.8.3 AC-3   ACCESS ENFORCEMENT

Control: The information system shall enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Additionally all information systems shall, at a minimum, enforce a discretionary access control (DAC) policy that:

a. Allows users to specify and control sharing by named individuals or groups of individuals, or by both;
b. Limits propagation of access rights; and
c. Includes or excludes access to the granularity of a single user.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, 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. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, Physical and Environmental Protection (PE)-3.

4.9 IMPLEMENTATION:

All information systems shall, at a minimum, enforce a discretionary access control policy that covers the requirements of AC-3(4). For periods processing, consider tailoring in [SC-4(2)]. Additional access enforcement controls apply to mobile computing devices, certain data as defined by the Data Owner, and Cross Domain Solution (CDS). See also Protection of

Information at Rest [SC-28], Access Control (AC) for Mobile Devices [AC-19], and CDS in Information Flow Enforcement [AC-4]. Access by Foreign Nationals-Information is not releasable to foreign nationals except as authorized by the respective service/agency.

Control Enhancements:

4.9.1.1 AC-3(2) ACCESS ENFORCEMENT |DUAL AUTHORIZATION

Control: The organization enforces dual authorization for all transfers of data from a classified computer network to removable media.

This includes the technical separation of roles (e.g., DTA and ISSM or designated representative etc.). Only trained DTAs are authorized to transfer data from a IS to removable media. Only ISSM and/or designated representatives are authorized to enable permissions to transfer data to removable media. This control supports insider threat mitigation.

Data transfer authorization enforcement can be performed by the organization, but should have technical separation of roles to support the organization's implemented dual authorization process.

Example of implementation meeting the spirit of AC-3(2): The organization policy states that appropriately trained Data Transfer/Trusted Download Agents are the only individuals authorized to transfer data from a classified system to removable media and only the ISSM and/or designated representatives are authorized to enable permissions to transfer removable media.

Supplemental Guidance: Dual authorization mechanisms require the approval of two authorized individuals in order to execute. Organizations do not require dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety. Dual authorization may also be known as two-person control. Related controls: Contingency Planning (CP)-9, Media Protection (MP)-6.

4.9.1.2 AC-3(4) ACCESS ENFORCEMENT |DISCRETIONARY ACCESS CONTROL

Control: The information system enforces discretionary access control to include or exclude access to the granularity of a single user who may be granted authorization to:
   a. Pass the information to any other subjects or objects;
   b. Grant its privileges to other subjects;
   c. Change security attributes on subjects, objects, the information system, or the information system's components;
   d. Choose the security attributes to be associated with newly created or revised objects; or
   e. Change the rules governing access control.

The assumption is that some user data/information in organizational information systems is not shareable with other users who have authorized access to the same systems.

The policy shall address at a minimum:
   a. Allows users to specify and control sharing by named individuals or groups of individuals, or by both[AC-3(4)(a)];
   b. Limits propagation of access rights [AC-3(4)(b)]; and
   c. Includes or excludes access to the granularity of a single user. [AC-3(4)(c)].

Supplemental Guidance: When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. This control enhancement can operate in conjunction with AC-3(3). A subject that is constrained in its operation by policies governed by AC-3(3) is still able to operate under the less rigorous constraints of this control enhancement. Thus, while AC-3(3) imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, AC-3(4) permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside of the control of the information system, additional means may be required to ensure that the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.

4.9.2 AC-4   INFORMATION FLOW ENFORCEMENT

Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers). These devices employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or provide message-filtering capabilities based on content (e.g., using key word searches or document characteristics). Within the environment, information flow control is provided by the infrastructure via the implementation of various boundary protection devices.

Supplemental 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. Control enhancements 3 through 22 primarily address cross-domain 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 (IT) products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

Information flow enforcement is addressed through the use of controlled interfaces (CI), including CDS, and assured file transfers (AFT)/trusted downloads. AFTs require data tracking logs for all transfers and a trained DTA.

Controlled Interface
A CI is a mechanism that facilitates adjudicating the security policies of different interconnected information systems (e.g., controlling the flow of information into or out of an interconnected system; often referred to as a guard). [CNSSI 4009]

Controlling the flow of information into an interconnected system helps preserve the integrity of the system, and the integrity and confidentiality of the information maintained and processed by the system. Controlling the flow of information out of the system helps preserve the confidentiality of the information leaving the system, and may protect the integrity of the receiving system.

Controlled interfaces that control the flow of information out of an IS are often employed to facilitate push technology, where the goal is to push information to an indirect user residing outside of the system perimeter (equipment responsibility demarcation), but within the system boundary (users).

The adjudication of integrity and confidentiality policies may be handled in a variety of ways. For example, a single CI may perform all of the confidentiality and integrity adjudication; or one CI may be employed for adjudicating confidentiality policies while another adjudicates integrity policies; or the adjudication of confidentiality and integrity policies may be distributed across a set of CI where each performs some subset of confidentiality and integrity policy adjudication.

While a CI is often implemented as a mechanism (or a set of mechanisms) separate from the systems it is intended to protect, this need not be the case. A CI can be constructed so that some of its functionality resides in the systems themselves. The term CI includes CDS, routers, firewalls, etc. The classification of the domains, to include the criteria to release data, is an indicator of what type of CI is required. See AC-4(20)

Trusted Download (TD)/Assured File Transfers
There are two types of data transfers: Low-to-High and High-to-Low. Documented and AO approved data transfer Low-to-High is defined as a transfer from a lower classification system to a higher classification system and also includes data transferred between two like security

domains, High-to-Low is defined as a transfer from a higher classification system to a lower classification system. It also includes a transfer between systems of the same classification with a differing set of programs, i.e., different security domains, for example, Conducting manual data transfers between security domains can be a time consuming, labor intensive process and must be done methodically and accurately to assure integrity of the source information, assure that only the data identified for transfer is transferred, prevent introduction of malicious software, and to prevent data spills. Careless methods, shortcuts, and untrained users have compromised sensitive and classified information vital to national security, mission success, and operational processes. TD/AFT procedures are established to mitigate the risks associated with all aspects of this activity and are conducted by individuals trained in the risks associated with transferring data between disparate security domains. The DTA is responsible for understanding the risks involved in data transfers and following the TD/AFT procedures to ensure any potential risk is managed during the download and transfer process. (Reference AT-3 for AFT/DTA training.) The subject matter expert (SME) is an individual knowledgeable of the program and the classification of information associated with it and is responsible for ensuring the file is reviewed and sanitized of all program-related data.

All new and reused media must be virus scanned with the latest definitions prior to starting an AFT.

Data Transfer Tracking
All data transfers (e.g., low to high, high to low) must be tracked to include date, originator making request, filename, file format, classification level, source and destination systems, and approver.

A **Low to High** transfer requires:
a. Log for transfers from a lower classified system (Secret or Top Secret) to a higher classified system, e.g., Secret to Top Secret Data transferred from an unclassified system must be logged, e.g., vendor software updates or antivirus definition.
b. Two virus/malware scans. The first scan is performed once the file(s) is downloaded to the media on the originating system; the second scan is performed on the media on the target system prior to uploading the file to the system. When possible, use virus/malware scanning products from different vendors.
c. Testing of the write protect mechanism. Once media is introduced on the High side, the capability to write to the media must be tested to ensure the media is write-protected. If the test fails and the media is written to on the High side, the media must be classified at the higher classification level.

A separate standalone system for scanning may be used if documented in the approved data transfer procedures.

High to Low transfer requires:
a. A log documenting date, originator making request, filename and format type (e.g.,.doc, .xls, .pdf), classification level, DTA who performed transfer, SME who performed review, originating system, target system, and approver.
b. Documented mission justification.
c. As a community best practice, use of an automated review tool in lieu of a manual transfer process (e.g., checklist)
d. AO approval for use of automated tools or a manual transfer process/checklist, to include any GCA requirements, as part of the SSP.

4.9.3 AC-5   SEPARATION OF DUTIES

Control: The organization:
   a. Separates at a minimum, duty of system administrators from audit administration functions as feasible;
   b. Documents separation of duties of individuals; and
   c. Defines information system access authorizations to support separation of duties.

Supplemental 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. Related controls: AC-3, AC-6, Physical and Environmental Protection (PE)-3, PE-4, Personnel Security (PS)-2.

The AO may authorize tailoring of this control based on risk identified to the information and/or operational environment. The ISSM must include justification for tailoring this control within the SSP.

Control Enhancements: None. References: None.

4.9.4 AC-6 LEAST PRIVILEGE

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 organizational missions and business functions.

The organization enforces the most restrictive set of rights/privileges or access needed by users for the performance of specific tasks.

Supplemental 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. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

For example, system administrators, security administrators, and database administrators perform functions that do not require use of their fully privileged account. They shall, therefore, use a separate general user account and are required to use that account when not performing privileged functions. [AC-6(2)] Individual email accounts should not be used when logged in as a privileged user.

Other examples of least privilege include restricting access to audit logs to security auditors, preventing general users from installing software, and/or limiting access to media drives to DTAs that have been trained.

In accordance with Insider Threat Mitigation Guidance, ISSMs will ensure that the number of privileged users is kept to a minimum and conduct a quarterly review of all privileged users and their associated permissions quarterly. The ISSM shall provide an annual review report to the AO.

Any changes to the privileged users shall also be reported to the AO. Note: DTAs are considered privileged users with limited, specific elevated privileges.

Control Enhancements:

4.9.4.1　AC-6(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Control: The organization explicitly authorizes access to systems and/or software that provide and security-relevant functions. (e.g., Universal Serial Bus (USB) ports, Input/Output (I/O) ports, Compact Disc (CD)/Digital Versatile Disk (DVD) drives, etc.). This control supports insider threat mitigation.

All classified information systems must technically enforce restrictions on the ability to write to removable media. By default, all write functionality must be disabled. Whenever access to writable removable media is necessary, the write functionality may be enabled, but this must be logged. After the write functions are completed, the write functionality must again be disabled and logged. Ensure media access is audited as indicated in AU-2.a.

Limiting access to security functions to a limited set of authorized personnel reduces the number of individuals able to perform security functions, such as configuring permissions, setting audit logs, etc. At a minimum, **all IS must technically enforce restrictions on the ability to write to removable media; (e.g., all CD/DVD write functionality must be disabled by default and enabled only when required for the execution of an approved data transfer).**

Supplemental 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. Related controls: AC-17, AC-18, AC-19.

An example of this is authorizing access to specific system endpoints, such as access to USB ports, CD/DVD drives, microphones, cameras, and least privilege on ability to make changes to port security implemented on switches. Additional roles on the network must also be considered.

All classified information systems must technically enforce restrictions on the ability to write to removable media. By default, all write functionality must be disabled. Whenever access to writable removable media is necessary, the write functionality may be enabled, but this must be logged. After the write functions are completed, the write functionality must again be disabled and logged.

4.9.4.2   AC-6(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

Control: The organization requires that users of information system accounts, or roles, with access to privileged functions, use non-privileged accounts or roles, when accessing non-system functions.

They shall, therefore, use a separate general user account and are required to use that account when not performing privileged functions. Requiring users with elevated privileges to use separate accounts enables more accurate audit of privileged user actions. **Organizations should also establish a separate privileged account specific to DTA activities**. This control supports insider threat mitigation.

Supplemental Guidance: This control enhancement limits exposure when operating from within privilege 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. Related control: PL-4.

4.9.4.3 AC-6(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

Control: The organization restricts privileged accounts on the information system to **absolute minimum number of privileged users needed to manage the system.** In addition, super-user/root privileges shall be limited to the maximum extent possible.

For example, not all privileged users will be granted full super-user/root access.

Supplemental 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. Related control: CM-6.

4.9.4.4 AC-6(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

Control: The organization:
   a. Reviews **at least annually** the privileges assigned to **privileged user accounts including DTA role** to validate the need for such privileges; and
   b. Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

The NISPOM, Change 2 requires organizations develop insider threat programs.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

4.9.4.5   AC-6(8) LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION

The information system prevents **software applications/programs** from executing at higher privilege levels than users executing the **application/program**.

Organizations shall maintain inventory of software in use and mechanism used to enforce and ensure this control.

Example: To maintain system integrity most systems restrict the ability of an application to install other software (including reinstalling itself). Windows users (from Vista on) are familiar with User Account Control (UAC) popup or the need to right click and "Run as Administrator" in order to install an application. Linux users are familiar with a "su" or "sudo" to root privilege to install applications.

The context of this enhancement is in the basic control where it states "or processes acting on behalf of users." This enhancement typically overlaps with and enables AC-6(1). Both Windows and Linux distinguish between normal user level privilege and privileged user privilege (admin and root).

Another example is the Windows registry editor that runs for all users, but only allows editing of the registry values authorized for each user.

Even for privileged users, it is not uncommon to find that the audit management and backup applications only execute for users in the assigned groups.

Some software requires privileged escalation by design, such as the UNIX password program; ensure AC-6(8) is tailored to document those programs, as applicable.

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

4.9.4.6   AC-6(9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS

The information system audits the execution of privileged functions.

Privileged functions have elevated permissions to access, or grant access to information. Accountability requires the ability to detect, trace, and audit privileged functions. The information system prevents all **applications/programs** from executing at higher levels than users executing the **application/program**. This control supports insider threat mitigation.

Supplemental 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). Related control: AU-2.

4.9.4.7   AC-6(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

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

Privileged functions have access beyond that of the typical user and may have greater ability to access administrative functions.

Supplemental 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. References: None.

4.9.5 AC-7   UNSUCCESSFUL LOGON ATTEMPTS

Control: The information system:
  a. Enforces a limit of **maximum of three** consecutive invalid logon attempts by a user during a fifteen (15) minute time period**; and**
  b. Automatically **locks the account/node until released by an administrator** when the maximum number of unsuccessful attempts is exceeded, when the account is supported locally; or if not supported locally, **after a period of not less than 15 minutes** when the maximum number of unsuccessful attempts is exceeded. (Includes the requirements of AC-7(1)).

Supplemental 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. Related controls: AC-2, AC-9, AC-14, IA-5.

If not supported locally, then the account/node shall be automatically locked for a minimum of 15 minutes.

4.9.6 AC-8   SYSTEM USE NOTIFICATION

Control: The information system:
  a. Displays to users the **Notice and Consent Banner** before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance and states that:
     (1) Users are accessing a U.S. Government information system;
     (2) Information system usage may be monitored, recorded, and subject to audit;
     (3) Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
     (4) Use of the information system indicates consent to monitoring and recording.
  b. Retains the notification message or banner on the screen until users acknowledge the

usage conditions and take explicit actions to log on to or further access the information system; and

c. For publicly accessible systems:
   (1) Displays system use information and prevents further activity on the information system unless and until the user takes positive action to acknowledge agreement by clicking on a box indicating "OK" 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.

Supplemental Guidance: 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. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.

Notice and Consent Banners: "Standard mandatory notice and consent banners must be displayed at logon to all ISs and standard mandatory consent notice and consent provisions will be included in all IS user agreements in accordance with applicable security controls and implementation procedures." The most current required text for the banner and user agreements is listed within the DAAPM. References: None.

4.9.7 AC-10 CONCURRENT SESSION CONTROL
Control: The information system limits the number of concurrent sessions for each **user** to **maximum of three sessions**. The concurrent sessions can be defined globally, by account type (e.g., privileged user), account or combination. This control may require third party software of development of a script.

Supplemental 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 a n d does not address concurrent sessions by single users via multiple system accounts. This control may require third party software or development of a script.

Control Enhancements: None. References: None.
4.9.8 AC-11 SESSION LOCK
Control: The information system:
   a. Prevents further access to the system by initiating a session lock after **not to exceed fifteen (15) 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.

Session locks (aka screen locks) shall be configured to require Authentication for reentry into the system. Systems supporting token-based authentication shall lock when the token is removed. All

users are required to logout of all systems at the end of each workday and for any extended absence (6 hours). Operational considerations may require exceptions to this requirement, e.g., operational testing of weapons systems or watch standing environments. This control also addresses unattended processing, which must be identified in the SSP specifying the functions and/or mission related tasks that must run as unattended processes.

Unattended Processing

Unattended processing is defined as automated processes executed/running on a user's behalf while no users are physically present in the area/facility. Unattended processes generally run after hours during the week or on weekends. Automated processes may include IT administrative functions (e.g., backups, scans) as well as mission-related tasks requiring additional network resources, e.g., executing complex algorithms. Open storage is approved based on physical authorization with regard to media, mission need, and risk. Unattended processing is approved by the AO based on system, mission justification, and environment.

Unattended processing must be captured in the SSP identifying the specific IT administrative functions and/or mission-related tasks that run as unattended processes. If possible, implement screen lock or appropriate prominently displayed signage.

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. Related control: AC-7.

Supplemental Guidance: Note: Operational considerations may require exceptions to this requirement. Exceptions must be approved in writing by the AO or designee. Session locks are not authorized in lieu of logout procedures. This control supports insider threat mitigation.

Control Enhancements:
4.9.8.1 AC-11(1)   SESSION LOCK | PATTERN-HIDING DISPLAYS
Control: The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

The information system session lock mechanism, when activated, shall hide screen content using **an unclassified pattern or image.** This control supports insider threat mitigation.

Supplemental 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. Ensure an unclassified image is displayed on the monitor to prevent unauthorized disclosure of classified information
References: Office of Management and Budget (OMB) Memorandum 06-16.

4.9.9 AC-12 SESSION TERMINATION
Control: The information system automatically terminates a user session **when the user logs out of the IS or removes the token**.

Supplemental 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.
Related controls: SC-10, SC-23.

Control Enhancements:
4.9.9.1   AC-12(1) SESSION TERMINATION | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS
Control: The information system:
   a. Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to all information **resources;** and
   b. Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

Supplemental Guidance: Information resources to which users gain access via authentication includes, for example, local workstations, databases, and password-protected websites/web-based services.

Logout messages for web page access, for example, can be displayed after authenticated sessions have been terminated. However, for some types of interactive sessions including, for example, file transfer protocol (FTP) sessions, information systems typically send logout messages as final messages prior to terminating sessions.
References: None.

4.9.10 AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
Control: The organization:
   a. Identifies that **no user actions** can be performed on the information system without identification or authentication consistent with organizational missions/business functions, and s**pecific AO authorization**; and
   b. Documents and provides supporting rationale in the SSP for the information system, user actions not requiring identification or authentication.

Supplemental Guidance: This control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. The organization may be required to implement compensatory measures.

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. Related controls: CP-2, IA-2.

Control Enhancements: None.
4.9.11 AC-16 SECURITY ATTRIBUTES
Control: The organization:
   a. Provides the means to associate classification, categories of information, and caveats 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 attributes (e.g., classification level, accesses, and handling caveat) in accordance with in accordance with IS contractual requirements IS; and
   d. Determines the permitted values for each of the established security attributes.

Supplemental Guidance: 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.

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. 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. Related controls: AC-3, AC-4, AC-6, AC-21, AU-2, AU-10, SC-16, MP-3.

Control Enhancements:

4.9.11.1 AC-16(5) SECURITY ATTRIBUTES | ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES

Control: The information system displays security attributes in human-readable form on each object that the system transmits to output devices to identify special dissemination, handling, or distribution instructions using human-readable, standard naming conventions.

Supplemental Guidance: Information system outputs include, for example, pages, screens, or equivalent. Information system output devices include, for example, printers and video displays on computer workstations, notebook computers, and personal digital assistants.

4.9.11.2 AC-16(6) SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION

Control: The organization allows personnel to associate, and maintain the association of **the appropriate level of classification, access and/or handling caveats** associated with files they create in accordance with the SCG or locally defined security policies.

For example, the contractor implements the appropriate classification, access, handling caveats for files (e.g., document, email, image, folder) they create in accordance with SCG or locally defined security policies.

Supplemental Guidance: This control enhancement requires individual users (as opposed to the information system) to maintain associations of security attributes with subjects and objects.

4.9.11.3 AC-16(7) SECURITY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION

Control: The organization provides a consistent interpretation of security attributes transmitted between distributed information system components.

Supplemental Guidance: In order to enforce security policies across multiple components in distributed information systems (e.g., distributed database management systems, and service-oriented architectures), organizations provide a consistent interpretation of security attributes that are used in access enforcement and flow enforcement decisions.

Organizations establish agreements and processes to ensure that all distributed information system components implement security attributes with consistent interpretations in automated access/flow enforcement actions.

4.9.12 AC-17 REMOTE ACCESS

Control: 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.

Supplemental 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. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, System and Information Integrity (SI)-4.

Access to an extension of an information system at an external location is not considered remote access. For the purpose of this control, system/network administration within the authorization boundary of the system, regardless of physical location, is not considered remote access. All remote access must be approved by the AO.

Control Enhancements:
4.9.12.1 AC-17(1) REMOTE ACCESS | AUTOMATED MONITORING / CONTROL
Control: The information system monitors and controls remote access methods.
All remote sessions and user activity shall be audited. This control supports insider threat mitigation.

Supplemental 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). Related controls: AU-2, AU-12. Additional related control: SI-4.

4.9.12.2 AC-17(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION
Control: The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-12, SC-13.

4.9.12.3 AC-17(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS
Control: The information system routes all remote accesses through a limited number of managed access control points (e.g., via an organizationally remote access server, such as a Citrix Server). This control is considered a National Security Systems (NSS) best practice.

Supplemental 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. Related control: SC-7.

4.9.12.4 AC-17(4) REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS
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. This control is considered an NSS best practice.

Supplemental Guidance: Related control: AC-6.

4.9.12.5 AC-17(6) REMOTE ACCESS | PROTECTION OF INFORMATION
Control: The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure. This control is considered an NSS best practice.
Supplemental Guidance: Related controls: AT-2, AT-3, PS-6.

4.9.12.6 AC-17(9) REMOTE ACCESS | DISCONNECT / DISABLE ACCESS
Control: The organization provides the capability to expeditiously disconnect or disable remote access to the information system no later than one hour after notification, 30 minutes of identification of an event or inactivity for low confidentiality or integrity impact; 20 minutes for moderate confidentiality or integrity impact; or 10 minutes for high confidentiality or integrity impact.

Supplemental Guidance: This control enhancement requires organizations to have the capability to rapidly disconnect current users remotely accessing the information system and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information systems.
References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.

4.9.13 AC-18 WIRELESS ACCESS
Control: The organization:
   a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access;
   b. Authorizes wireless access to the information system prior to allowing such connections; and
   c. Proactively monitor for unauthorized wireless connections, including scanning for unauthorized wireless points at least quarterly.

Supplemental Guidance: Wireless technologies include microwave, packet radio (Ultrahigh Frequency (UHF)/Very High Frequency (VHF)), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., Extensible Authentication Protocol (EAP)/Transport Layer Security (TLS), PEAP), which provide credential protection and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.

This control applies even if no wireless is authorized in the facility. For example, wireless is prohibited and implementation guidance should include that users are instructed/reminded during initial and annual refresher training that wireless access and wireless devices are prohibited [AC-18.a].

In certain situations, wireless signals may radiate beyond the confines and control of organization-controlled facilities. As a result, wireless technologies are generally prohibited from use in facilities. Exceptions may include wireless devices without memory that convey no meaningful data (e.g., personal wearable devices, remote control devices for audio/visual presentations, and infrared (IR) and Bluetooth mice). Any exceptions shall be documented and approved by the AO and cognizant ISSP/SCA [AC-18.b] to include limiting wireless capabilities within the facility boundary. Such exceptions could also warrant Certified TEMPEST Technical Authority (CTTA) evaluation.

CTTA involvement if required by contract.

The risks associated with personally-owned wireless technologies used in medical devices must also be assessed. The ISSM/ISSO will work in concert with AO, as appropriate, to allow necessary medical devices to the greatest extent possible, yet within the acceptable risk envelope as determined by the AO.

Control Enhancements:

4.9.13.1 AC-18(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION
Control: If applicable, the information system protects wireless access to the system using authentication of both users and devices as appropriate; (e.g., devices to wireless networks and users to enterprise services and encryption). This control is considered an NSS best practice.
Supplemental Guidance: Related controls: SC-8, SC-13.

4.9.13.2 AC-18(3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING
Control: The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

Document and ensure wireless is disabled or removed from devices entering the facility, e.g., televisions, portable electronic devices, printers.
Supplemental Guidance: Related control: AC-19.

4.9.13.3 AC-18(4) WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS
Control: The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

This control supports insider threat mitigation.

Supplemental Guidance: Organizational authorizations to allow selected users to configure wireless networking capability are enforced in part, by the access enforcement mechanisms employed within organizational information systems. Related controls: AC-3, SC-15.

4.9.14 AC-19 ACCESS CONTROL FOR MOBILE DEVICES
Control: The organization:
  a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and

   b. Authorizes the connection of mobile devices to organizational information systems.

Mobile devices include portable computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices, also referred to as Portable Electronic Device (PED). A PED is any easily transportable, personally-owned or government issued, electronic device that has the capability to record, copy, store, and/or transmit data, digital images, video, and/or audio.

Examples of a PED include, but are not limited to, pagers, laptop computers, cellular telephones, radios (amplitude modulation/frequency modulation, satellite), compact discs players, cassette players and recorders, Personal Digital Assistant (PDA) (e.g., palmtops, BlackBerrys, iPads), digital audio devices (e.g., MP3 players, iPods), cameras, camcorders, calculators, electronic book readers (e.g., Kindles, Nooks, Neos), digital picture frames, and electronic watches with input capability and/or reminder recorders. See also [MP-4] and [MP-5].

All personnel shall:
 a. Be subject to monitoring of unauthorized connections;
 b. Obtain approval from the **AO** to carry the PED into and out of facilities;
 c. Obtain a property pass authorizing the carrying of government-procured PEDs into and out of facilities. Ensure the authorized inventory control label such as the unified industries incorporated (UII) number is "physically attached" to the government-issued PED. The make, model, serial number, and UII of the PED shall be included on the property pass;
 d. Maintain this property pass with the government-procured PED at all times; and
 e. Protect government-issued PEDs from unauthorized access and theft. Report any violation or suspected violation to the DSS and the ISSM.

See the Media Protection (MP) section, for policy and procedures related to removable storage media. Reference the MP section for media control including PED removable media.

Purchase of government PEDs shall conform to the same policies and procedures as all other IT equipment. See the System and Services Acquisition (SA) section for additional information on mobile devices.

Supplemental 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 t hi s 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. Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4.

PEDs for Classified Use.
PEDs authorized for classified use represent a special class of government-owned mobile devices authorized with mission justification for its use. The ISSM assigns responsibilities for the use of these PEDs with the Closed Area information-and establishes procedures to control their use and accountability to ensure classified information is protected from unauthorized disclosure.

Control Enhancements:
4.9.14.1 AC-19(5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION
Control: The organization employs NSA-approved encryption to protect the confidentiality and integrity of information on **all mobile devices authorized to connect to the organization's IS**.

PEDs that contain classified or controlled unclassified information (CUI) information must be encrypted with an NSA or approved encryption standard.

Supplemental 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. Related controls: MP-5, SC-13, SC-28. References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.

4.9.15 AC-20 USE OF EXTERNAL INFORMATION SYSTEMS
Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
  a. Access the information system from external information systems; and
  b. Process, store, or transmit organization-controlled information using external information systems.

An external information system may be interconnected system/service. Providers of external information systems should provide the ISSM with an external.

Supplemental 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, (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 is 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, 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.

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.usa.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. Related controls: AC-3, AC-17, AC-19, CA-3, PL-4, SA-9.

Control Enhancements:
4.9.15.1 AC-20(1) USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE
Control: The organization permits authorized individuals to use an interconnected external 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.

An approved connection agreement is in place with the organization hosting the External Information System. This may be accomplished via the establishment of an approved ISA. If the

interconnecting systems have the same AO, an ISA is not required. This control supports insider threat mitigation.

Supplemental Guidance: This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., 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. Related control: CA-2.

4.9.15.2 AC-20(2) USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES

Control: The organization shall limit the use of organization-controlled portable storage devices by authorized individuals on external information systems.

AO approval is required. This control supports insider threat mitigation.

Supplemental 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.

4.9.15.3 AC-20(3) USE OF EXTERNAL INFORMATION SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES

Control: The organization prohibits the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information unless specifically approved by the AO/AO Representative.

Supplemental Guidance: Non-organizationally owned devices include devices owned by other organizations (e.g., federal/state agencies) and personally owned devices. There are risks to using non-organizationally owned devices. In some cases, the risk is sufficiently high as to prohibit such use. In other cases, it may be such that the use of non-organizationally owned devices is allowed but restricted in some way. Restrictions include:
   a. Requiring the implementation of organization-approved security controls prior to authorizing such connections;
   b. Limiting access to certain types of information, services, or applications;
   c. Using virtualization techniques to limit processing and storage activities to servers or other system components provisioned by the organization; and
   d. Agreeing to terms and conditions for usage.

For personally owned devices, organizations consult with the Office of the General Counsel regarding legal issues associated with using such devices in operational environments, including, for example, requirements for conducting forensic analyses during investigations after an incident.

4.9.15.4   AC-20(4) USE OF EXTERNAL INFORMATION SYSTEMS | NETWORK ACCESSIBLE STORAGE DEVICES

Control: The organization prohibits the use of fined network accessible storage devices in external information systems, **unless specifically approved by the AO**.

Supplemental Guidance: Network accessible storage devices in external information systems include, for example, online storage devices in public, hybrid, or community based systems. References: FIPS Publication 199.

4.9.16 AC-21 INFORMATION SHARING

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; and
   b. Employs automated or manual review process to assist users in making information sharing/collaboration decisions.

Supplemental 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. Related control: AC-3.

AC-21 is related to AC-3; additional detail may be provided in AC-21 that addresses assisting users in meeting AC-16 requirements, e.g., Access Look-up tool.

A sharing partner may be an individual or group on the IS, or external to the IS, e.g., sharing is being done in a circumstance where the IS cannot enforce appropriate sharing controls, e.g., video teleconferences (VTCs), phone conversations, and fax transmittals. The organization will use an approved mechanism to ensure informed security decisions are made, preventing inadvertent disclosures

Control Enhancements:
 5.19 AC-22 PUBLICLY ACCESSIBLE CONTENT (Removed from DSS Baseline)

4.9.17 AC-23 DATA MINING PROTECTION

Control: The organization employs data mining prevention and detection for Program information to adequately detect and protect against data mining.

Data mining prevention and detection techniques include, for example: (i) limiting the types of responses provided to database queries; (ii) limiting the number/frequency of database queries to increase the work factor needed to determine the contents of such databases; and (iii) notifying organizational personnel when atypical database queries or accesses occur.

Supplemental Guidance: Data storage objects include, for example, databases, database records, and database fields. This control focuses on the protection of organizational information from data mining while such information resides in organizational data stores. In contrast, AU-13

focuses on monitoring for organizational information that may have been mined or otherwise obtained from data stores and is now available as open source information residing on external sites, for example, through social networking or social media websites.

Control Enhancements: None. References: None
4.10   AWARENESS AND TRAINING

4.10.1 AT-1   SECURITY AWARENESS AND TRAINING (AT) POLICY AND PROCEDURES
Control: The organization:
  a.   Develops, documents, and disseminates to all personnel:
      (1) A security 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 awareness and training policy and associated security awareness and training controls; and
  b.   Reviews and updates the current:
      (1) Security awareness and training policy **annually**; and
      (2) Security awareness and training procedures **at least annually**.

Supplemental 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. Related control: PM-9.

Control Enhancements: None.
References: NIST Special Publications 800-12, 800-16, 800-50, 800-100.
4.10.2 AT-2   SECURITY AWARENESS TRAINING
Control: The organization provides basic security awareness training to information system users (including managers, and senior executives):
  a.   As part of initial training for new users;
  b.   When required by information system changes; and
  c.   At least annually thereafter.

Security awareness training will be conducted:
  a.   During in-processing: site specific information will be briefed based on the mission and requirements of the job;
  b.   Upon receipt of a USERID and authenticator: the Privileged User, ISSO or their alternate will brief the user on his/her IA responsibilities;
  c.   Annually, as part of refresher training and awareness: classroom training, briefings, computer-based training, or seminars will be conducted and participation/completion documented to ensure all users understand and comply with IA training requirements; and
  d.   Annual refresher and awareness training may also be delivered through staff meetings, online delivery systems, or similar venues and documented in accordance with Security

Training Records; as required, due to policy or regulatory violations and lessons learned from incident handling and response.

Supplemental Guidance: Organizations determine the appropriate content of security awareness training and security 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 to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events. Related controls: AT-3, AT-4, PL-4.

The purpose of security awareness training is to sensitize the user to the threats and vulnerabilities of national security information systems, and inform the user of the need to protect information and the systems that process, transmit and/or store information.

Control Enhancements:
4.10.2.1 AT-2(2) SECURITY AWARENESS | INSIDER THREAT
Control: The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Indicators of insider threat can include behaviors such as job dissatisfaction, unexplained financial resources, consistent violations of organizational policies, etc. Additional information on insider threat indicators training can be found at: http://www.cdse.edu/catalog/insider-threat.html

Supplemental 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. Related controls: PL-4, PM-12, PS-3, PS-6.

References: C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); Executive Order 13587; NIST Special Publication 800-50.

4.10.3 AT-3   ROLE-BASED SECURITY TRAINING
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.   At least annually thereafter.

All users shall receive initial and at least annual General User training; while users assigned to positions requiring privileged access shall receive, in addition, Privileged User training.

Supplemental Guidance: Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations 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 organizational information security programs. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.

General User Training

General User training will include, but is not limited to, the following:
    a. The organization's policy for protecting information and IS including the rules of behavior, which specify acceptable user actions to include explicit restrictions on the use of social networking sites, posting information on commercial websites, and sharing information system account information.
    b. The organization's policy regarding appropriate use of IS resources as specified in the User Agreement and the possible repercussions of misuse or abuse.
    c. How to protect the physical area, media, and equipment (e.g., door access, alarms, care of hard drives, CDs).
    d. How to protect authenticators and operate the applicable system security features (e.g., setting access control rights to files created by the user).
    e. How to recognize and report suspected security violations and incidents.
    f. Understanding the importance of classification and control marking compliance.
    g. Basic actions to take in the event of a data spill. Reference: [IR-2] Privileged User Training.

Privileged user training will include, but is not limited to, the following:
    a. Completion of General User training.
    b. Rules of behavior, as they apply to the privileged user.
    c. A thorough understanding of the organization's policy for protecting information and systems, to include change management, and the roles and responsibilities of various organizational units with which they may have to interact.
    d. The organization's policy regarding appropriate privileged use of IS resources and the possible repercussions of misuse or abuse.
    e. How to protect the system (e.g., maintenance and backup, care of system media, protection and retention of audit logs, endpoint security).
    f. How to protect passwords, or other authentication devices/mechanisms, and be familiar with operating system security features and technical safeguards of the system.
    g. How to recognize and report potential security vulnerabilities, threats, security violations, or incidents.
    h. Technical actions to take in the event of a data spill. Reference [IR-2].
    i. How to implement and use specific IA products provided by the organization.
    j. IA training in compliance with the NISPOM and DAAPM Prior to obtaining privileged

user system access credentials:
   (1) Complete the applicable Privileged User Access Training; see also Security Training [AT-3].
   (2) Provide the training completion certificate and privileged user agreement to the ISSM.

Assured File Transfer Training (See also [AC-4].)

An individual performing data transfers is commonly referred to as a DTA. The DTA is performing a security-relevant function in providing endpoint security during a data transfer. DTAs must be identified in writing. AFT training for DTAs will include, but is not limited to the following:
   a. Training in the use of data review and sanitization tools (automated and manual).
   b. Working knowledge of the Security Classification Guide.
   c. File formats permissible for AFT.
   d. Authorized media formats and marking requirements.
   e. Program management approval and Security process compliance review.

Control Enhancements:

4.10.3.1 AT-3(2) SECURITY TRAINING | PHYSICAL SECURITY CONTROLS

Control: The organization provides ISSM with initial and annual training in the employment and operation of physical security mechanisms or when sufficient changes are made to physical security systems. This control supports insider threat mitigation.

Supplemental Guidance: Physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures). Organizations identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training. Related controls: PE-2, PE-3, PE-4, PE-5.

4.10.3.2 AT-3(4) SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

Control: The organization provides training to its personnel on indicators in order to recognize suspicious communications and/or anomalous behavior in organizational information systems. (e.g., receiving a suspicious email, an unexpected web communication, etc.).

Supplemental Guidance: A well-trained workforce provides another organizational safeguard that can be employed as part of a defense-in-depth strategy to protect organizations against malicious code coming in to organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email. Personnel are also trained on how to respond to such suspicious email or web communications (e.g., not opening attachments, not clicking on embedded web links, and checking the source of email addresses). For this process to work effectively, all organizational personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in organizational information systems can potentially provide early warning for the presence of malicious code. Recognition of such anomalous behavior by organizational personnel can supplement automated malicious code detection and protection tools and systems employed by organizations.

4.10.4 AT-4 SECURITY TRAINING RECORDS

Control: The organization:

    a.   Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

    b. Retains individual training records for **a minimum of five years**.

Training records shall contain, at a minimum, the following elements:

    a.   User name.
    b. Name of training.
    c.   Date of training (initial and refresher).
    d. Type of training (classroom, one-on-one, online CBT, briefing, etc.).

Initial training records must contain signatures. Refresher training may be documented through user-initialed attendance rosters, e-mail acknowledgments, USERIDs captured through online content delivery systems, or other similar user acknowledgments. In addition, organizations shall maintain training records.

Supplemental Guidance: Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14.
References: None.

4.10.5 AU-1   AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization:

    a.   Develops, documents, and disseminates to ISSO, ISSM, FSO, designated users, and auditing 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 the current:

        (1) Audit and accountability policy **at least annually**; and

        (2) Audit and accountability procedures **at least annually**.

Supplemental 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. Related control: PM-9.

An audit trail is a record of events. Audit trails may be limited to specific events, or they may encompass all activities on a system. A computer system might have several audit trails, each focused on a particular type of activity, such as detecting security violations, performance problems, and design and programming flaws in applications. Periodic reviews of audit logs may be useful for:

    a.   Detecting unauthorized access to information.

b.   Establishing a culture of responsibility and accountability.
c. Reducing the risk associated with inappropriate accesses (behavior may be altered when individuals know they are being monitored).
d. Providing forensic evidence during investigations of suspected and known security incidents and breaches to privacy, especially if sanctions against a workforce member, business associate, or other contracted agent will be applied.
e. Tracking disclosures of sensitive and/or classified information.
f. Responding to concerns regarding unauthorized access.
g. Evaluating the overall effectiveness of policy and user education regarding appropriate access and use of information (comparing actual activity to expected activity and discovering where additional training or education may be necessary to reduce errors).
h. Detecting new threats and intrusion attempts.
i. Identifying other potential security related incidents.
j. Addressing compliance with regulatory requirements.

An audit trail enables a security practitioner to trace the history of activities on an information system. The audit trail provides information about additions, deletions, or modifications to data within a system. Audit trails enable the enforcement of individual accountability by allowing a reconstruction of events. Like monitoring, one purpose of an audit trail is to assist in problem identification and resolution. Any unusual activity or variation from the established procedures should be identified and investigated. Audit can assist in:
a. **Accountability** – Log data can identify what accounts are associated with certain events. This information then can be used to highlight where training and/or disciplinary actions are needed. Accountability is the system's capability to determine the actions and behaviors of a single individual within a system and to identify that particular individual. Audit trails and logs support accountability.
b. **Reconstruction** – Log data can be reviewed chronologically to determine what was happening both before and during an event. For this to happen, the accuracy and coordination of system clocks are critical. To accurately trace activity, clocks need to be regularly synchronized to a central source to ensure that the date/time stamps are in synch.
c. **Intrusion Detection** – Unusual or unauthorized events can be detected through the review of log data, assuming that the correct data is being logged and reviewed. The definition of what constitutes unusual activity varies, but can include failed login attempts, login attempts outside of designated schedules, locked accounts, port sweeps, network activity levels, memory utilization, key file/data access, etc.
d. **Problem Detection** – In the same way that log data can be used to identify security events, it can be used to identify problems that need to be addressed. For example, investigating causal factors of failed jobs, resource utilization, trending and so on.

The audit capability should be automated where feasible and provide adequate on-line or off-line storage of audit information separate from data files. If automated audit collection is not supported, use of manual audits must be documented in the SSP. The AO's ATO must specify approval to implement manual audits.

Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.
4.10.6 AU-2 AUDIT EVENTS
Control: The organization:
a. Determines that the information system is capable of auditing the following events:
(1) Successful and unsuccessful attempts to access, modify, or delete privileges, security

objects, security levels, or categories of information (e.g. classification levels).

(2) Successful and unsuccessful logon attempts;

(3) Privileged activities or other system level access;

(4) Starting and ending time for user access to the system;

(5) Concurrent logons from different workstations, Successful and unsuccessful accesses to objects;

(6) All program initiations;

(7) All direct access to the information system;

(8) All account creations, modifications, disabling, and terminations; and

(9) All kernel module load, unload, and restart.

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;

d. Determines that the information system is capable of auditing the following events at minimum:

(10) Authentication events:

(a) Logons (Success/Failure).

(b) Logoffs (Success).

(11) Security Relevant File and Objects events:

(a) Create (Success/Failure).

(b) Access (Success/Failure).

(c) Delete (Success/Failure).

(d) Modify (Success/Failure).

(e) Permission Modification (Success/Failure).

(f) Ownership Modification (Success/Failure).

(g) Export/Writes/downloads to devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure).

(h) Import/Uploads from devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure).

(12) User and Group Management events:

(a) User add, delete, modify, disable, lock (Success/Failure)

(b) Group/Role add, delete, modify (Success/Failure).

(13) Use of Privileged/Special Rights events:

(a) Security or audit policy changes (Success/Failure).

(b) Configuration changes (Success/Failure).

(c) Admin or root-level access (Success/Failure).

(d) Privilege/Role escalation (Success/Failure).

(e) Audit and security relevant log data accesses (Success/Failure).

(f) System reboot, restart and shutdown (Success/Failure).

(g) Print to a device (Success/Failure).

Supplemental 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, Personal Identity Verification (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. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.

Determine, based on current threat information and on-going assessment of risk, which events are to be audited within the information system.

Ensure system console activities are audited as well as access to pertinent objects other than security-relevant, e.g., mission, program.

Tailoring audit collection requirements related to specific applications is recommended

Control Enhancements:
4.10.6.1 AU-2(3) AUDIT EVENTS | REVIEWS AND UPDATES
Control: The organization reviews and updates the audited events annually and based on situational awareness of threats, vulnerabilities.

The auditable events baseline list, as defined above, shall be reviewed annually or as policy and procedures dictate changes are required. The review shall include coordination with other organizational entities requiring audit-related information (e.g., Incident Response (IR), Counterintelligence) to enhance mutual support and to help guide the selection of auditable events. This control supports insider threat mitigation.

4.10.7 AU-3 CONTENT OF AUDIT RECORDS
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.

Specifically, audit records shall contain, at a minimum, the following content:
   a. USERID.
   b. Type of event/action.
   c. Success or failure of event/action.
   d. Date.
   e. Time.
   f. Terminal or workstation ID.

  g. Entity that initiated event/action.
 h. Entity that completed event/action.
 i. Remote Access.

If manual audit collection is approved by the AO, the audit records shall contain, at a minimum, the following content:
 a. Date.
 b. Identification of the user.
 c. Time the user logs on and off the system.
 d. Function(s) performed.
 e. Terminal or Workstation ID.

Manual audit logs may be used to record the transmission of any data over a fax connected to a secure voice line (e.g., Secure Terminal Equipment (STE)). These logs will be maintained for one year and must include the following information:
 a. Sender's name, organization and telephone number.
 b. Date and time of fax transmission.
 c. Classification level of the information.
 d. Recipient's name, organization and telephone number.

Supplemental 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). Related controls: AU-2, AU-8, AU-12, SI-11.

4.10.7.1 AU-3(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION
Control: The information system generates audit records containing the following additional information such as:
 a. 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.
 b. 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.
 c. Specifically, audit records shall contain, at a minimum, the following content:
  (1) USERID.
  (2) Type of event/action.
  (3) Success or failure of event/action.
  (4) Date.
  (5) Time.
  (6) Terminal or Workstation ID.
  (7) Entity that initiated event/action.
  (8) Entity that completed event/action.
  (9) Remote access.

4.10.8 AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates audit record storage capacity.

Proper audit storage capacity is crucial to ensuring the ongoing logging of critical events. The information system must be configured to allocate sufficient log record storage capacity so that it will not become exhausted. See also AU-5(1).

Supplemental Guidance: Organizations consider 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. Related controls: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4.

Control Enhancements:
4.10.8.1 AU-4(1) AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE
Control: The information system off-loads audit records **based on organizational requirements** onto a different system or media than the system being audited.

Organizations should assign a frequency or threshold capacity when audit records are off-loaded. Related control: AU-9(2).

Supplemental Guidance: Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred. References: None.

4.10.9 AU-5   RESPONSE TO AUDIT PROCESSING FAILURES
Control: The information system:
   a. Alerts **Designated organizational officials, (ISSM, ISSO, and system administrator)** in the event of an audit processing failure; and
   b. Takes the following additional actions: **at a minimum, record any audit processing failure in the audit log**.

System should alert **designated organizational officials: ISSM, ISSO, and system administrator**. For IS that are not capable of providing a warning, procedures for a manual method must be documented.

Tactical/deployable information systems may be developed without all the features and security controls of standard information systems. Audit requirements for these systems should be reviewed for mission impact. For example, failure of the audit process should not interfere with continued normal operation of a mission critical system.

Supplemental Guidance: Audit processing failures include 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. Related controls: AU-4, SI-12.

At a minimum, record any audit processing failure in the audit log. System should alert a system administrator and/or ISSM/ISSO. For IS that are not capable of providing a warning, procedures for a manual method must be documented.

Control Enhancements:

4.10.9.1 AU-5(1) RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY

Control: The information system provides a warning to ISSM and IA personnel immediately when allocated audit record storage volume reaches **(75 percent) of repository maximum audit record storage capacity.**

This control supports insider threat mitigation.

Auditing processing failures include, e.g. software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Supplemental Guidance: Organizations may have multiple audit data storage repositories distributed across multiple information system components, with each repository having different storage volume capacities.

4.10.10 AU-6   AUDIT REVIEW, ANALYSIS, AND REPORTING

Control: The organization:
   a. Reviews and analyzes information system audit records **at least weekly** for indications of **any inappropriate or unusual activity**; and
   b. Reports vulnerabilities to ISO, ISSM and FSO.

The purpose of this review is to verify all pertinent activity is properly recorded and appropriate action has been taken to correct and report any identified problems. These reviews shall be documented in either an electronic or manual log. Organizationally defined personnel or roles may include ISO, ISSM and/FSO.

Supplemental 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 voice over internet protocol (VoIP). Vulnerabilities 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. Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, Risk Assessment (RA)-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.

Control Enhancements:

4.10.10.1   AU-6(1) AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION

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.

Supplemental Guidance: Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits. Related controls: AU-12, PM-7.

4.10.10.2   AU-6(3) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES

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

Supplemental 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. Related controls: AU-12, IR-4.

4.10.10.3   AU-6(4) AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS

Control: The information system provides the capability to centrally review and analyze audit records from multiple components within the system.

Supplemental Guidance: Automated mechanisms for centralized reviews and analyses include, for example, Security Information Management products. Related controls: AU-2, AU-12.

4.10.10.4   AU-6(5) AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES

Control: The organization integrates analysis of audit records with analysis of vulnerability scanning information; performance data; and/or information system monitoring information; and Program-defined data/information collected from other sources to further enhance the ability to identify inappropriate or unusual activity.

Supplemental Guidance: This control enhancement does not require vulnerability scanning, the generation of performance data, or information system monitoring. Rather, the enhancement requires that the analysis of information being otherwise produced in these areas is integrated with the analysis of audit information. Security Event and Information Management System tools can facilitate audit record aggregation/consolidation from multiple information system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans and correlating attack detection events with scanning results.

Correlation with performance data can help uncover denial of service attacks or cyber-attacks resulting in unauthorized use of resources.

Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations. Related controls: AU-12, IR-4, RA-5.

4.10.10.5   AU-6(8) AUDIT REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS

Control: The organization performs a full text analysis of audited privileged commands in a physically distinct component or subsystem of the information system, or other information system that is dedicated to that analysis.

Supplemental Guidance: This control enhancement requires a distinct environment for the dedicated analysis of audit information related to privileged users without compromising such information on the information system where the users have elevated privileges including the capability to execute privileged commands. Full text analysis refers to analysis that considers the full text of privileged commands (i.e., commands and all parameters) as opposed to analysis that considers only the name of the command. Full text analysis includes, for example, the use of pattern matching and heuristics. Related controls: AU-3, AU-9, AU-11, AU-12.

4.10.10.6   AU-6(9) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES

Control: The organization correlates information from nontechnical sources with audit information to enhance organization-wide situational awareness**.**

Supplemental Guidance: Nontechnical sources include, for example, human resources records documenting organizational policy violations (e.g., sexual harassment incidents, improper use of organizational information assets). Such information can lead organizations to a more directed analytical effort to detect potential malicious insider activity. Due to the sensitive nature of the information available from nontechnical sources, organizations limit access to such information to minimize the potential for the inadvertent release of privacy-related information to individuals that do not have a need to know. Thus, correlation of information from nontechnical sources with audit information generally occurs only when individuals are suspected of being involved in a security incident. Organizations obtain legal advice prior to initiating such actions. Related control: AT-2.

4.10.10.7   AU-6(10) AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT

Control: The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Supplemental Guidance: The frequency, scope, and/or depth of the audit review, analysis, and reporting may be adjusted to meet organizational needs based on new information received. References: None.

4.10.11 AU-7 AUDIT REDUCTION AND REPORT GENERATION

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 ordering of audit records.

Supplemental 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. Related control: AU-6.

Control Enhancements:
4.10.11.1   AU-7(1) AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING
Control: The information system provides the capability to process audit records for events of interest based on selectable event criteria.

Supplemental 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, Internet 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. Related controls: AU-2, AU-12.
References: None.

4.10.12 AU-8 TIME STAMPS
Control: The information system:
   a. Generates date and time stamps from internal system clocks for audit records; and
   b. Records time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

Supplemental Guidance: Time stamps generated by the information system include date and time. Time is commonly expressed in UTC, a modern continuation of 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. Related controls: AU-3, AU-12.

Control Enhancements:
4.10.12.1   AU-8(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE
Control: The information system:
   a. Compares the internal information system clocks at least every 24 hours with an organization-defined authoritative time source e.g., Domain Controller, US Naval Observatory time server; and
   b. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than **the organizationally defined granularity in AU-8**.

This control is considered an NSS best practice.

Supplemental Guidance: This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

4.10.13AU-9   PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Audit information shall be handled and protected at the same security level of the information system from which it originated until reviewed and a determination is made of the actual classification.

Supplemental 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. Related controls: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6.

Control Enhancements:

4.10.13.1   AU-9(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

Control: The organization shall limit access to audit functionality to only a small subset of privileged users.

Where applicable, access shall be further restricted by distinguishing between privileged users with audit-related privileges and privileged users without audit-related privileges to improve audit integrity. Limiting the users with audit-related privileges helps to mitigate the risk of unauthorized access, modification, and deletion of audit information. This control supports insider threat mitigation.

Supplemental 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. Related control: AC-5.

When feasible, limit access to the audit role. Computer security managers and system administrators or managers should have access for review purposes; however, security and/or administration personnel who maintain logical access functions may have no need for access to audit logs.

References: None.

4.10.14AU-11 AUDIT RECORD RETENTION

Control: The organization retains audit records for a minimum of 1 year or one inspection cycle whichever is greater to provide support after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental 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, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6.

The purpose of audit retention is to provide support for after-the-fact investigations of security incidents and to meet regulatory and organization information retention requirements. Although most requests for audit information from law enforcement (LE) or inspectors general (IGs) are within the one year mark, audit records going back five years provide historic information that is frequently used in espionage cases for damage assessment purposes to determine what the (alleged) perpetrator may have accessed.

Control Enhancements:
4.10.14.1   AU-11(1) AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY

Control: The organization employs **retention of technology to access audit records for the duration of the required retention period** to ensure that long-term audit records generated by the information system can be retrieved.

Supplemental Guidance: Measures employed by organizations to help facilitate the retrieval of audit records include, for example, converting records to newer formats, retaining equipment capable of reading the records, and retaining necessary documentation to help organizational personnel understand how to interpret the records.
References: None.

4.10.15 AU-12 AUDIT GENERATION
Control: The information system:
   a. Provides audit record generation capability for the auditable events defined in AU-2(a) at all information systems and network components;
   b. Allows designated personnel to select which auditable events are to be audited by specific components of the information system; and
   c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Supplemental 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. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.

Control Enhancements:
4.10.15.1   AU-12(1) AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL
Control: The information system compiles audit records from information systems audible devices into a system-wide (logical or physical) audit trail that is time-correlated to **the tolerance defined in AU-8 and AU-12**.

The AU-12(1) organization-defined IS components is a subset of the organization-defined components in AU-12 focused on correlated and centralizing specific audits.

Supplemental Guidance: Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances. Related controls: AU-8, AU-12.

4.10.15.2   AU-12(3) AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS

Control: The information system provides the capability for organization-defined individuals to change the auditing to be performed on information system components based on organization-defined selectable event criteria

The information system binds the identity of the information producer to the information and provides the means for authorized individuals to determine the identity of the producer of the information.

Supplemental Guidance: This control enhancement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed, for example, near real-time, within minutes, or within hours. Related control: AU-7.
References: None.

4.10.16 AU-14 SESSION AUDIT *(Removed from DSS Baseline)*

4.10.16.1   AU-14(1) SESSION AUDIT | SYSTEM START-UP *(Removed from DSS Baseline)*

4.10.16.2   AU-14(2) SESSION AUDIT | CAPTURE/RECORD AND LOG CONTENT *(Removed from DSS Baseline)*

4.10.16.3   AU-14(3) SESSION AUDIT | REMOTE VIEWING/LISTENING *(Removed from DSS Baseline)*

4.10.17   AU-16 CROSS-ORGANIZATIONAL AUDITING *(Removed from DSS Baseline)*

4.10.17.1   AU-16(1) CROSS-ORGANIZATIONAL AUDITING | IDENTITY PRESERVATION

Control: The organization requires that the identity of individuals be preserved in cross-organizational audit trails.

Supplemental Guidance: This control enhancement applies when there is a need to be able to trace actions that are performed across organizational boundaries to a specific individual.

4.10.17.2 AU-16(2) CROSS-ORGANIZATIONAL AUDITING | SHARING OF AUDIT INFORMATION

Control: The organization provides cross-organizational audit information to specifically-identified organizations based on sharing agreements as identified in an ISA, SLA, or MOA.

Supplemental Guidance: Because of the distributed nature of the audit information, cross-organization sharing of audit information may be essential for effective analysis of the auditing being performed. For example, the audit records of one organization may not provide sufficient information to determine the appropriate or inappropriate use of organizational information resources by individuals in other organizations. In some instances, only the home organizations of individuals have the appropriate knowledge to make such determinations, thus requiring the sharing of audit information among organizations.
References: None.

4.11 SECURITY ASSESSMENT AND AUTHORIZATION

4.11.1 CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Control: The Defense Security Service shall: develop, document, and disseminate to all personnel:
   a. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
   b. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
   c. Reviews and updates the current:
      (1) Security assessment and authorization policy **annually;** and
      (2) Security assessment and authorization procedures **at least annually**.

Supplemental 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. Related control: PM-9.

Control Enhancements: None.
References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100.
4.11.2 CA-2 SECURITY ASSESSMENTS
Control: The Defense Security Service shall:
   a. Develop 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 **at least annually, or as stipulated in the organization's continuous monitoring**

program 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 to ISSP/**SCA and the AO Representative**.

The initial security assessment is performed by the ISSM and determines the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. ISSM will forward IS certification statement to DSS as part of the security package within OBMS.

A recurring security assessment is conducted as part of the continuous monitoring requirements to ensure the IS complies with the documented security requirements and that the security of the IS, as authorized, is maintained throughout its life cycle. Self-assessments will be routinely conducted by the ISSM. Security assessments may be routinely conducted as required.

For the NISP and for all IS under the purview of the AO/AO Representative, the Security Assessment Plan is embodied in the information provided in the SSP, and the Security Control Assessment Procedures, all of which must be reviewed and approved by the SCA/ISSP and AO.

Information revealing specific vulnerabilities (other than the known vulnerabilities of widely available commercial products) and the compiled results of vulnerability analyses for all systems shall be classified in accordance with the Security Classification Guide. If not explicitly required, the result shall be considered Unclassified. If SCG describes vulnerabilities as classified, contact your AO-designated representative for handling instructions.

4.11.2.1 CA-2(1) SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS

Control: The organization employs assessors or assessment teams to conduct security control assessments at a **level of impartiality determined by the AO.**

Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness. Security assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization.

Supplemental 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. DSS meets this control.

4.11.3 CA-3   SYSTEM INTERCONNECTIONS

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 ISAs.

Organizations shall identify any connections of an information system to an external information system in the SSP and ensure connections from the information system to external information systems are authorized through the use of an ISA. An external information system is an information system or component that is outside the authorization boundary as defined in the SSP. (Reference AC-20.)

Organizations typically have no direct control over the security controls or security control effectiveness for these external systems or components. Organizations shall monitor all information system connections on an ongoing basis to verify enforcement of the security requirements. If the interconnecting systems have the same AO, an ISA is not required, although one may still be beneficial.

When a need arises to connect two different IS operating at different security classification levels, the connection is referred to as a cross domain connection. Any cross domain connection must be identified first to the Service or Agency Cross Domain Support Element. All cross domain connections shall comply with the security controls identified STIG.

The direct connection of any information system to an external network is prohibited.

Supplemental 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. Authorizing officials determine the risk associated with information system connections dend the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements.

Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. 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. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.

Direct connection means that an information system cannot connect to an external network without the use of an approved boundary protection device (e.g., firewall or cross domain device) that mediates the communication between the system and the network.

4.11.3.1 CA-3(1) SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS *(Removed from DSS Baseline)*

Control Enhancements:
4.11.3.2 CA-3(2) SYSTEM INTERCONNECTIONS | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS
Control: The organization prohibits the direct connection of a classified, national security system processing to an external network without the use approved boundary protection devices and AO approval.

Supplemental Guidance: Organizations typically do not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (i.e., information flows) between classified national security systems and external networks. In addition, approved boundary protection devices (typically managed interface/cross-domain systems) provide information flow enforcement from information systems to external networks.

4.11.3.3 CA-3(5) SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS
Control: The organization employs **deny-all, permit-by-exception** policy for allowing **all systems** to connect to external information systems.

Supplemental 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. Related control: CM-7. References: FIPS Publication 199, NIST Special Publication 800-47, and CA-4 SECURITY CERTIFICATION.

4.11.4 CA-5   PLAN OF ACTION AND MILESTONES
Control: The organization:

a. Develops a plan of action and milestones for the information system 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 existing plan of action and milestones **at least quarterly** based on the vulnerabilities from security controls assessments, security impact analyses, and continuous monitoring activities.

POA&Ms are the authoritative management tool used by the organization (including the AO, SCA) to detail specific program and system level security weaknesses, remediation needs, the resources required to implement the plan, and scheduled completion dates.

The POA&M is initiated based on vulnerabilities and recommendations from the SAR, or as a minimum, providing that information via the SAR to the ISSM.

The ISSM shall describe the planned tasks for correcting weaknesses and addressing any residual vulnerability. The POA&M shall identify:

a. Tasks to be accomplished with a recommendation for completion either before or after information system implementation.

b. Resources required accomplishing the tasks.

c. Any milestones in meeting the tasks, to include percentage completed.

d. Scheduled completion dates for the milestones.

e. Status of tasks (completed, ongoing, delayed, planned).

The POA&M is used by the AO and SCA to monitor the progress in mitigating any vulnerabilities. POA&M entries are required even when weaknesses or deficiencies are remediated during the assessment or prior to the submission of the authorization package to the AO.

Supplemental Guidance: Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB. Related controls: CA-2, CA-7, CM-4, PM-4.

Control Enhancements:
References: OMB Memorandum 02-01; NIST Special Publication 800-37.
4.11.5 CA-6   SECURITY AUTHORIZATION (DSS Internal Process)

4.11.6 CA-7   CONTINUOUS MONITORING
Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of a IA controls and metrics to be monitored;

b. Establishment of monitoring frequency for each security control;

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 the organization and the information system to

appropriate organizational officials at least annually, or whenever there is a significant change to the system or the environment in which the system operates**.**

Supplemental 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 risk-based 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. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.

Continuous monitoring of security controls using automated support tools (e.g. SCAP with associated benchmarks conducted quarterly) facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system.

The ultimate objective of continuous monitoring is to achieve a state of ongoing authorization where the AO maintains sufficient knowledge of the current security state of the information systems under their purview (including the effectiveness of the security controls employed within and inherited by the system). This information is used to determine whether continued operation maintains an acceptable level of risk in accordance with the AO. If a formal reauthorization action is required, the organization maximizes the use of security and risk-related information produced during the continuous monitoring and ongoing authorization processes.

Continuous monitoring assists organizations with ongoing updates to SSPs and POA&Ms and minimizes the level of effort required for subsequent security assessment activities.

Control Enhancements:
4.11.6.1 CA-7(1) CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT
Control: The organization employs assessors or assessment teams to perform an objective assessment to monitor the security controls in the information system on an ongoing basis.

Supplemental Guidance: Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process.

To achieve such impartiality, assessors should not:

a.   Create a mutual or conflicting interest with the organizations where the assessments are being conducted;

b. Assess their own work;

c. Act as management or employees of the organizations they are serving; or

d. Place themselves in advocacy positions for the organizations acquiring their services.

4.11.7 CA-9   INTERNAL SYSTEM CONNECTIONS

Control: The organization:

a. Authorizes internal connections of information system components to the information system; and

b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

Supplemental Guidance: This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration. Related controls: AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4.

4.12   CONFIGURATION MANAGEMENT

Control Enhancements:

4.12.1 CM-1   CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to all stakeholders in the configuration management process.

(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 the current:

(1) Configuration management policy **annually;** and

(2) Configuration management procedures **annually.**

Program-specific policies and procedures must be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the CM-1 control.

Supplemental 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. Related control: PM-9.

Control Enhancements: None.
References: NIST Special Publications 800-12, 800-100.
4.12.2 CM-2   BASELINE CONFIGURATION
Control: Organizations must develop, document, and maintain the current baseline configuration for all information systems under their purview to include, but not limited to, workstations, servers, network components and mobile devices.

A baseline configuration describes the approved configuration of an information system including all hardware (manufacturer, model and serial number or unique identifier), software (manufacturer, name, version number), and firmware components (manufacturer, name and version number), how various security controls are implemented, how the components are interconnected, and the physical and logical locations of each.

Supplemental 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. Related controls: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.

Baseline configuration includes the documentation required in CM-6 (including configuration settings and hardening applied to the system and software), CM-7 (including requirements for whitelisting software) and CM-8 (hardware inventory).

Control Enhancements:
4.12.2.1 CM-2(1) BASELINE CONFIGURATION | REVIEWS AND UPDATES
Control: The organization reviews and updates the baseline configuration of the information system:
   a. At least annually;
   b. When required due to baseline configuration changes or as events dictate such as changes due to-Changes that modify the security structure; and
         (1) Operating system changes (e.g., Windows XP to Windows 7).
         (2) Major software version upgrades (e.g., Office 2007 to Office 2010).
         (3) Addition to servers.
         (4) Modification to system ports protocols and services (PPS).
         (5) Major vulnerabilities discovered after assessment and/or authorization.
         (6) Changes to the confidentiality, integrity, or availability requirements (e.g., changing from a moderate impact level to high impact level).
         (7) Changes in system encryption methods.

(8)   Changes in interconnections.

(9) Changes to operating environment (e.g. External information System introduces media capability, introduction of Voice over internet Protocol (VOIP) (classified or unclassified, foreign nationals move in next door, system is relocated).

(10) Significant increased threat increasing the organization/sites residual risk. Minor and non-security relevant hardware and software changes to information systems do not require assessment retesting. These upgrades require an administrative update to the SSP. Examples of changes that only require administrative updates include:

(a) Non-security relevant software version updates and/or upgrades.

(b) Addition of identical workstation type with approved image to an authorized system.

(c) Replacement of failed servers/system components with identical spares

(d) Replacement of hardware drives/tape back-up.

c. As an integral part of information system component installations and upgrades. Supplemental Guidance: Related control: CM-5.

4.12.2.2 CM-2(2) BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY/CURRENCY

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Supplemental Guidance: Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM-8(2) for organizations that choose to combine information system component inventory and baseline configuration activities. Related controls: CM-7, RA-5.

4.12.3 CM-3 CONFIGURATION CHANGE CONTROL

Control: The Organization **must**:

a. Determine the types of changes to the information system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

c. Document configuration change decisions associated with the information system;

d. Implement approved configuration-controlled changes to the information system;

e. Retain records of configuration-controlled changes to the information system for **the life of the system;**

f. Audit and reviews activities associated with configuration-controlled changes to the information system; and

g. Coordinate and provide oversight for configuration change control activities through establishment of a group of individuals with the collective responsibility and authority to review and approve proposed changes to the IS that convenes as defined in the local SSP and when there is a significant change to the system or the environment in which

the system operates. This is a function overseen by the ISSM and/or ISSO/AO.

Examples of these types of changes include:
   a.   Changes that modify the security support structure.
   b.   Operating system changes (e.g., Windows XP to Windows 7).
   c.   Major software version upgrades (e.g., Office 2007 to Office 2010).
   d.   Addition of software not previously approved for systems.
   e.   Addition of servers or new server function.
   f.   Modification to system PPS.
   g.   Major vulnerabilities discovered after assessment and/or authorization.
   h.   Changes to the confidentiality, integrity, or availability requirements (e.g. changing from a moderate impact level to a high impact level).
   i.   Changes in system encryption methods.
   j.   Changes to interconnections.
   k.   Changes to operating environment (e.g. External Information System introduces media capability; introduction of Voice over Internet Protocol (VoIP) (classified or unclassified); foreign nationals move in next door; system is relocated).
   l.   Significant increased threat increasing the organization/site's residual risk.

Minor and non-security relevant hardware and software changes to information systems do not require assessment retesting. These upgrades require an administrative update to the SSP. Examples of changes that only require administrative updates include:
   a.   Non-security relevant software version updates and/or upgrades.
   b.   Addition of identical workstation type with approved image to an authorized system.
   c.   Replacement of failed servers/system components with identical spares.
   d.   Replacement of hard drives/tape back-up.

The addition of any server/workstation identified in the paragraph above requires the ISSM/ISSO to review the test results pre and post connection to ensure the information system has been configured in accordance with the approved artifacts. If in doubt on the significance of a change, the SCA shall be contacted to determine whether a change is significant.

When feasible, a Configuration Control Board acts as a check and balance on configuration change activity, assuring that proposed changes are held to organizationally defined criteria (e.g., scope, cost, impact on security) before being implemented. CM-3 g. organization-defined values should establish the   element responsible for approving change. **A CCB can be as big or small as it needs to be for the information system environment that it supports.**

Since the ISSM is responsible for halting practices dangerous to security, the ISSM shall have authority to veto any proposed change he/she believes to be detrimental to security. In cases of disagreement, the change shall be postponed while the ISO or ISSM contacts the AO's office for resolution. Reference: CA-6.

Modifying, relocating, or reconfiguring the hardware of any computer system must be approved by the CCB for each site. Hardware will not be connected to any system/network without the express written consent of the ISSM/ISSO and the CCB.

Modifying, installing, or downloading any software on any computer system may affect system authorization and must be evaluated and approved by the ISSM/ISSO with the local CCB.

Supplemental 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. Related controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.

All hardware and software changes to IS must go through a configuration change control process. Configuration change control is the documented process for managing and controlling changes to the configuration of an IS.

Security Relevant: any hardware or software that is "security enforcing," "security supporting," or "security non-interfering" which can affect an IS's configuration, functionality, or users' privileges, and has the potential to change the risk imposed on the IS.

    a. **Security Enforcing** – Operating System (OS), access control applications, audit applications, device control applications, second party applications that perform IA, account management, anti-virus, firewall; capable of making changes to the security substructure of the system: modifies a user's account or changes permissions on objects such as enforcing DAC, Mandatory Access Control (MAC), Network Access Control (NAC).

    b. **Security Supporting** – Impacts a security process or procedures: e.g., software used to perform technical review for AFT; software that is only used by privileged users of the system in the performance of their duties; removing a backup server which may affect availability; code or script that authenticates the user and determines authorization.

    c. **Security Non-Interfering** – Does not enforce or support any aspect of the system security policy, but due to its presence inside the security boundary, e.g., code running a privileged hardware mode within the OS, risk is elevated.

Significant security-relevant changes will require assessment and may require re-authorization of the information system. A concept of operations or revised SSP will be submitted to the AO for authorization outlining the implementation and assessment process.

Documented AO authorization is required prior to implementing a security-relevant change, examples (not all-inclusive) include:

    a. Changes that modify the security support structure.
    b. Operating system changes (e.g., Windows 7 to Windows 10).
    c. Security Relevant software version upgrades (e.g., Update to Microsoft Office beyond TD/AFT tool capabilities, firmware update for security appliances).
    d. Addition of security relevant software not previously approved for the systems.
    e. Addition of new server function.
    f. New hardware models.
    g. Modification to system PPS.

     h.   Major vulnerabilities discovered after assessment and/or authorization.
  i.   Changes to the confidentiality, integrity, or availability requirements (e.g., changing from a moderate impact level to high impact level).
  j.   Changes in system encryption methods.
  k. Changes to interconnections.
  l.   Changes to operating environment (e.g., external information system introduces media capability; introduction of Voice over Internet Protocol (VoIP) (classified or unclassified); foreign nationals move in next door; system is relocated).
  m. Significant increased threat increasing the organization/site's residual risk.

Minor and non-security relevant hardware and software changes to information systems may require AO authorization. These upgrades require an administrative update to the SSP. Examples of non-security-relevant changes include:
  a. Non-security relevant software version updates and/or upgrades.
  b. Addition of identical workstation type with approved image to an authorized system.
  c. Replacement of failed servers/system components with identical spares.
  d. Replacement of hard drives/tape back-up.

The addition of any server/workstation identified in the paragraph above requires the ISSM/ISSO to review the test results pre and post connection to ensure the information system has been configured in accordance with the approved artifacts. If in doubt on the significance of a change, the SCA shall be contacted to determine whether a change is significant.

Control Enhancements:
4.12.3.1 CM-3(4) CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE
Control: The organization requires an information security representative to be a member of the CCB. Usually, the ISSM or his/her designated representative shall serve as a voting member of the CCB. Since the ISSM is responsible for halting practices dangerous to security, the ISSM shall have authority to veto any proposed change he/she believes to be detrimental to security. In cases of disagreement, the change shall be postponed while the ISO or ISSM contacts the AO's office for resolution.

Supplemental Guidance: Information security representatives can include, for example, senior agency information security officers, information system security officers, or information system security managers. Representation by personnel with information security expertise is important because changes to information system configurations can have unintended side effects, some of which may be security-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security state of organizational information systems. The configuration change control element in this control enhancement reflects the change control elements defined by organizations in CM-3.

ISSM responsibilities include serving as a member of the CCB.

4.12.3.2 CM-3(6) CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT
Control: The organization ensures that cryptographic mechanisms (public key, private key, etc.) used to provide all security safeguards are documented in the configuration management policy.

Supplemental Guidance: Regardless of the cryptographic means employed (e.g., public key, private key, shared secrets), organizations ensure that there are processes and procedures in place to effectively manage those means. For example, if devices use certificates as a basis for identification and authentication, there needs to be a process in place to address the expiration of those certificates. Related control: SC-13. References: NIST Special Publication 800-128.

4.12.4 CM-4 SECURITY IMPACT ANALYSIS
Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

The organization must maintain records of analysis of changes to the information system.

Security impact analysis is the deliberate consideration of the impact of a change on the security state of the information system. ISs are typically in a constant state of change. It is important to understand the impact of changes on the functionality of existing security controls. Security impact analysis must be incorporated into the documented configuration change control process. The ISSM/ISSO shall be involved in determining if a configuration change has a security impact. Factors considered in assessing software risk involve:

  a. Importation of malicious content: This is essentially a supply chain issue. Although we perceive that US sources are less likely to target the US, with multi-national firms and commercial open source, software (like hardware) comes from everywhere. That said, most of the repositories attempt to be malware free.
  b. Importation of vulnerable content: This factor relates to code quality including software assurance that the libraries used by applications are updated and that latent vulnerabilities in the executables are addressed/mitigated/removed.
  c. Remediation of functional or security deficiencies in operational software: This factor addresses effective sustainment to determine if the developer addresses identified vulnerabilities in a timely manner. It's not uncommon to have open source firms have patches posted in a few days where the commercial firms may lag for months. When developers and vendors abandon products (for various reasons), it can leave the consumer with orphan or zombie software. It can take deep pockets to pay for sustainment and delay an end-of-life deadline.
  d. Legal compliance: Licensing, copyrights, and intellectual property rights vary dependent on the software type, e.g., open source software, commercial off-the-shelf (COTS).
  e. Costs of the four factors above: Cost is often linked to platform and applications. For example, open source software is more common in the *nix environments (e.g., UNIX, LINUX), than in Windows, where the greatest cost tends to be for sustainment and licensing.

Hardware tends to follow a similar process with an additional focus on whether a device contains non-volatile memory and malicious content.

Systems with moderate and high integrity are required to have a test environment. Integrity low systems should consider impact of the change to their operational environment and ensure the change is implemented in the least disruptive manner.

If the security impact analysis results in significant security-relevant changes, documented approval is required from the AO in accordance with CM-3. Reference CA-6.

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Supplemental Guidance: Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, and Information System Security Managers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the change 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. Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.

Control Enhancements:
4.12.5 CM-5 ACCESS RESTRICTIONS FOR CHANGE
Control: The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

The organization permits only qualified and authorized individuals (privileged) to access information   systems for purposes of initiating changes, including upgrades and modifications. These access   restrictions enforce configuration control to the information system. The organization documents physical access restrictions   associated with changes to the information system in the configuration management policy.

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.

Supplemental 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).

Access restrictions for change represent the enforcement side of security configuration management. Configuration change control is a process for funneling changes to an IS through a managed process;   however, without access restrictions, there is nothing preventing someone from implementing changes outside the process. Access restrictions are a mechanism to enforce configuration control processes by controlling who has access to the IS to make changes.

Organizations are responsible for conducting scans or audits to validate configuration changes were implemented as intended and for supporting after-the-fact actions if unauthorized changes to the IS are detected. Related controls: AC-3, AC-6, PE-3. Control Enhancements:

4.12.5.1 CM-5(5) ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES

Control: The organization:

a. Limits developing/integrator privileges to change information system components (hardware, software, and firmware) and system-related information within a production or operational environment; and
b. Ensure the ISSM Reviews and reevaluates privileges **at least annually**.

Supplemental Guidance: 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. Related control: AC-2.

4.12.5.2 CM-5(6) ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES

The organization limits privileges to change software resident within software libraries.

Supplemental Guidance: Software libraries include privileged programs. Related control: AC-2. References: None.

4.12.6 CM-6 CONFIGURATION SETTINGS

Control: The organization must:

a. Establishes and documents configuration settings for information technology products employed within the information system using **security configuration or implementation guidance** 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 **guidance** in the System Security Plan; and
d. Develop, document, Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental 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 (USG) Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The 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. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4.

Control Enhancements:
4.12.7 CM-7 LEAST FUNCTIONALITY
Control: The organization must:
   a. Document in the security plan, essential capabilities which the information system must provide. The organization configures the information system to provide only those documented essential capabilities; and
   b. Prohibits or restricts the use of ports, protocols, and services using least functionality. Ports will be denied access by default, and allow access by exception as documented in the system security plan.

Least functionality helps to minimize the potential for introduction of security vulnerabilities and includes, but is not limited to, disabling or uninstalling unused/unnecessary OS functionality, protocols, ports, and services, and limiting the software that can be installed and the functionality of that software.

Supplemental 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. Related controls: AC-6, CM-2, RA-5, SA-5, SC-7.

Control Enhancements:

4.12.7.1 CM-7(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

Control: The organization must:

   a. Reviews the information system annually to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and

   b. Disables ports, protocols, and services within the information system deemed to be unnecessary (documented in the SSP CM-7).

Supplemental 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. Related controls: AC-18, CM-7, IA-2.

4.12.7.2 CM-7(2) LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION

Control: The information system prevents program execution by disabling or uninstalling unused/unnecessary OS functionality, protocols, ports, and services, and limiting the software that can be installed and the functionality of that software.

Organizations shall configure information systems and components to disable the capability for automatic execution of code (e.g. Auto Run, AutoPlay). This control supports insider threat mitigation.

Systems prevent program execution from organizationally specific locations: (e.g., removable media, temporary directory, a shared network drive, etc.). Supplemental guidance: none. Related controls: CM-8, PM-5.

4.12.7.3 CM-7(3) LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE

Control: Organizations shall obtain and ensure compliance with the latest guidance regarding ports, protocols, and services when applicable.

Supplemental Guidance: Organizations use the registration process to manage, track, and provide oversight for information systems and implemented functions, ports, protocols, and services.

4.12.7.4 CM-7(5) LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING

Control: The organization:

   a. Identifies develops and maintains an approved software list to execute on the information system. (Change to this list is managed within CM-3.);

   b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and

   c. Reviews the list of authorized software programs **at least quarterly and updates as required**.

The organization must maintain an audit trail of the review and update.

Supplemental Guidance: The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. In addition to whitelisting, organizations consider serifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions.

Verification of white-listed software can occur either prior to execution or at system startup. Related controls: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.

4.12.8 CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

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;
      (4) Includes a local hardware list providing as a minimum, type, make, model, quantity, serial number; and
      (5) Reviews and updates the information system component inventory **at least annually.**

The IS component inventory is a list of the physically identifiable components within an IS. The inventory must be available for review and audit by designated organizational officials.

Each IS component should be associated with only one IS, and every item in the IS component inventory should fall within the authorization boundary of a single IS).

Supplemental 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. Related controls: CM-2, CM-6, PM-5.

Control Enhancements:

4.12.8.1 CM-8(2) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE

Control: The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components, when feasible.

Supplemental Guidance: Organizations maintain information system inventories to the extent feasible. Virtual machines, for example, can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. This control enhancement can be satisfied by the implementation of CM-2(2) for organizations that choose to combine information system component inventory and baseline configuration activities. Related control: SI-7.

4.12.8.2 CM-8(3) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

Control: The organization, **when required:**
   a. Employs automated mechanisms continuously 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: Documents

and   implements a process to take action to disable network access by unauthorized software, hardware, and firmware components, isolate the components, and/or notify the ISSO and ISSM and others as the local organization deems appropriate. The organization must maintain an audit trail of actions taken upon detection of unauthorized software, hardware, and firmware components.

Supplemental 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. Related controls: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.

4.12.9 CM-9 CONFIGURATION MANAGEMENT PLAN

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.

A Configuration Management Plan is a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems. Organizations are responsible for developing a CM Plan for all information systems under their purview. The plan must define CM roles, responsibilities, processes and procedures. It must further define the configuration items for the IS and establish a process for managing the configuration of the configuration items throughout the system development life cycle.

ISO responsibilities include:
   a. Documenting the CM process when new IS are under development, being procured, or delivered for operation. An integral part of CM is the System Authorization process. Therefore, it is imperative that AOs or designees be advised of CM decisions. This will ensure systems are fielded or modified within acceptable risk parameters and the latest security technology is being incorporated into system designs.

ISSM responsibilities include:
   a. Ensuring development and implementation of procedures in accordance with CM policies and procedures for authorizing the use of hardware/software on an IS;
   b. Ensuring all additions, changes or modifications to hardware, software, or firmware are documented and that security relevant changes are coordinated, via the SCA, with the AO or appropriately delegated individual; and
   c. Serving as a voting member on the CCB.

Supplemental 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. Related controls: CM-2, CM-3, CM-4, CM-5, CM-8, SA-10.

Control Enhancements:
4.12.10 CM-10 SOFTWARE USAGE RESTRICTIONS
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.

Software use within an environment can make licensing difficult, but system specific controls that are in place to ensure licensing is properly managed are required.

Supplemental Guidance: Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs. Related controls: AC-17, CM-8, SC-7.

Software use within an environment can make licensing difficult, but system specific controls that are in place to ensure licensing is properly managed are required.

Control Enhancements:
4.12.10.1 CM-10(1) SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE
Control: The organization establishes the following restrictions on the use of open source software in the DAAPM:
   a. Open source software may only be used if specifically approved by the ISSM and the organization meets all licensing issues associated with the software.

Supplemental Guidance: Open source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open source software is that it provides organizations with the ability to examine the source code. However, there are also various licensing issues associated with open source software including, for example, the constraints on derivative use of such software. References: None.

4.12.11 CM-11 USER-INSTALLED SOFTWARE
Control: The organization:
    a. Establishes policies governing the installation of software by users (e.g. user agreements, CM Plan, etc.);
    b. Define and document the methods employed to enforce the software installation policies; and
    c. Monitors policy compliance quarterly.

Supplemental 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 organization-developed 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. Related controls: AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4.

Control Enhancements:
4.12.11.1   CM-11(2) USER-INSTALLED SOFTWARE | PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS
Control: The information system prohibits user installation of software without explicit privileged status.

Supplemental Guidance: Privileged status can be obtained, for example, by serving in the role of system administrator. Related control: AC-6. References: None.

4.13   CONTINGENCY PLANNING
Control: Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. Contingency planning generally includes one or more of the following approaches to restore disrupted services:
    a. Restoring information systems using alternate equipment.
    b. Performing some or all of the affected business processes using alternate processing (manual) means (typically acceptable for only short-term disruptions).
    c. Recovering information systems operations at an alternate location (typically acceptable for only long–term disruptions or those physically impacting the facility).
    d. Implementing appropriate contingency planning controls based on the information system's security impact level.

Information system contingency planning represents a broad scope of activities designed to sustain and recover critical system services following an emergency event. Information system contingency planning fits into a much broader security and emergency management effort that includes organizational and business process continuity, disaster recovery planning, and incident management. Ultimately, organizations use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's information systems, mission/business functions, personnel, and the facility. Because there is an inherent relationship between an information system and the mission/business process it supports, there must be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

Continuity and contingency planning are critical components of emergency management and organizational resilience but are often confused in their use. Continuity planning normally applies to the mission/business itself; it concerns the ability to continue critical functions and processes during and after an emergency event. Contingency planning normally applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency. Cyber Incident Response Planning is a type of plan that normally focuses on detection, response, and recovery to a computer security incident or event.

In general, universally accepted definitions for information system contingency planning and the related planning areas have not been available. Occasionally, this leads to confusion regarding the actual scope and purpose of various types of plans. To provide a common basis of understanding regarding information system contingency planning, this section identifies several other types of plans and describes their purpose and scope relative to information system contingency planning. Because of the lack of standard definitions for these types of plans, the scope of actual plans developed by organizations may vary from the descriptions below. This guide applies the descriptions and references in controls below to security and emergency management-related plans. The plans listed are in alphabetical order, and do not imply any order of importance.

The focus of this Contingency Planning section is information system contingency planning.

Plan Type	Purpose	Scope	Plan Relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining mission/ business operations while recovering from a significant disruption.	Addresses mission/ business functions at a lower or expanded level from Continuity of Operations (COOP) mission-essential functions.	Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-mission-essential functions.

Continuity of Operations Plan	Provides procedures and guidance to sustain an organization's mission essential functions at an alternate site for up to 30 days; mandated by federal directives.	Addresses mission-essential functions at a facility; information systems are addressed based only on their support of the mission-essential functions.	Mission-essential functions focused plan that may also activate several business unit-level BCPs, Information System Contingency Plans (ISCPs), or Disaster Recovery Plans (DRPs), as appropriate.
Crisis Communications Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system-focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of national critical infrastructure components, as defined in the National Infrastructure Protection Plan.	Addresses critical infrastructure components that are supported or operated by an agency or organization.	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets.
Cyber Incident Response Plan	Provides procedures for mitigating and correcting a cyber-attack, such as Denial of Service (DoS), Distributed Denial of Service (DDoS), exfiltration, etc., which may be executed by a virus, worm, Trojan horse or other malicious software (malware).	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	Information system-focused plan that may activate an ISCP or DRP, depending on the extent of the attack.
Disaster Recovery Plan	Provides procedures for relocating information systems operations to an alternate location.	Activated after major system disruptions with long term effects.	Information system-focused plan that activates one or more ISCPs for recovery of individual systems.

Information System Contingency Plan	Provides procedures and capabilities for recovering an information system.	Addresses single information system recovery at the current or, if appropriate, alternate location.	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP.
Occupant Emergency Plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property from damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not mission/business process or IS-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

4.13.1 CP-1   CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization:

   a.   Identify personnel responsible for Contingency Planning. This can be found in the approved System Security Plan. Contingency Planning Process and Procedures will be disseminated to appropriate personnel.

   b.   Create a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. A&A process manual and NIST 800-34 can be used as guidance. Create procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

   c.   Reviews and updates the current:
      (1) Contingency planning policy **at least annually**; and
      (2) Contingency planning procedures **at least annually**.

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the CP-1 control. For additional information on the types of contingency plans, review the section in the DAAPM.

Supplemental 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. Related control: PM-9.

Control Enhancements: None.

References: Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100.

4.13.2 CP-2 CONTINGENCY PLAN

Control: The organization:

    a. Develops a contingency plan for the information system that:
- (1) Identifies essential missions and business functions and associated contingency requirements;
- (2) Provides recovery objectives, restoration priorities, and metrics;
- (3) Addresses contingency roles, responsibilities, assigned individuals with contact information;
- (4) Addresses maintaining essential 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;
- (6) Is reviewed and approved by ISSM/FSO annually;
- (7) Distributes copies of the contingency plan to all stakeholders identified in the contingency plan via an information sharing capability;
- (8) Coordinates contingency planning activities with incident handling activities;
- (9) Reviews the contingency plan for the information system **at least annually**;
- (10) 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;
- (11) Communicates contingency plan changes to stakeholders identified in the contingency plan; and
- (12) Protects the contingency plan from unauthorized disclosure and modification.

The availability impact level drives the level of contingency required for the system. The Information System Contingency Plan may be either a separate document specific to the IS, included in the SSP, or may be incorporated into the Continuity of Operations Plan. ISCP development is the responsibility of the ISSM.

The mission owner or ISO determine to what lengths the ISSM/ISSO should go to ensure a contingency plan is in place, e.g., relocation of users/team/crew, hot backup, warm backup, backup media stored offsite, additional measures beyond backing up the data.

The plan must define and describe specific responsibilities of designated staff or positions to facilitate the recovery and/or continuity of essential system functions. The ISCP consists of a comprehensive description of all actions to be taken before, during, and after a disaster or emergency condition along with documented and tested procedures. The ISCP helps to ensure critical resources are available and facilitates the continuity of operations in an emergency situation.

Supplemental 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 process 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. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

Control Enhancements:
4.13.3 CP-3 CONTINGENCY TRAINING
Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:
    a. Within 60 days of assuming a contingency role or responsibility;
    b. When required by information system changes; and
    c. Annually or as defined in the contingency plan thereafter.

Supplemental 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. Related controls: AT-2, AT-3, CP-2, IR-2.

Control Enhancements:
4.13.4 CP-4   CONTINGENCY PLAN TESTING
Control: The organization:
    a. Tests the contingency plan for the information system annually using full scale contingency plan testing or functional/tabletop exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan;
    b. Documents and reviews the contingency plan test/exercise results; and
    c. Initiates the corrective actions, if needed.

It is recommended to conduct table top testing the first year and full scale testing on an annual basis.

Supplemental 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. Related controls: CP-2, CP-3, IR-3.

Results of documented tests should be retained for one year or one assessment cycle whichever is longer.

4.13.5 CP-7   ALTERNATE PROCESSING SITE

Control: The organization, as required:

a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential mission/business functions. The organization will define the time period consistent with recovery time and recovery point objectives for essential mission/business functions to permit the transfer and redemption of organization-defined information system operations at an alternate processing site when the primary processing capabilities are unavailable;

b. Ensures that equipment and supplies required to resume operations are available at the alternate processing site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption;

c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site; and

d. Develops alternate processing site agreements (e.g., MOA/MOU) that contain priority-of-service provisions in accordance with the organization's availability requirements.

Supplemental 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. Related controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6.

This control is likely to be tailored out if the system availability impact level is low.

4.13.6 CP-9   INFORMATION SYSTEM BACKUP

Control: The organization must:

a. Conducts backups of user-level information contained in the information system weekly;

b. Conducts backups of system-level information in the information system weekly;

c. Conduct backups of information system documentation including security-related documentation as required by system baseline configuration changes in accordance with the contingency plan; and

d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

The ISO shall develop backup plans for all information systems. Backup plans must be coordinated with the ISSM/ISSO and included in the ISCP. Backup plans should consider data-production rates and data-loss risks. The areas of risk that should be identified and planned for include, but are not limited to:

a.   Loss of power.
b. Loss of network connectivity.
c. Loss or corruption of data.
d. Facility disruptions, such as loss of air conditioning, fire, flooding, etc.

Backup procedures should reflect the risk from media loss. If a hard disk were damaged, lost or contaminated in some way, the disk backups, coupled with periodic incremental backups between full backups, would allow for the restoration of the data. "Active backups" should be maintained for disks that contain often-used applications.

Backup information must be protected to ensure its confidentiality and integrity. Digital signatures and cryptographic hashes can be employed to protect the integrity of information system backups. Reference SC-13, Cryptographic Protection. An organizational assessment of risk guides the use of encryption for protecting backup information. Reference SC-28, Protection of Data at Rest.

Supplemental 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. Related controls: CP-2, CP-6, MP-4, MP-5, SC-13.

Besides preventing data loss, backups of information for archiving purposes allow for proper on-line storage management.

This control may be tailored out.

4.13.7 CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

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.

Organizations shall ensure all backup and restoration hardware, firmware and software are adequately protected.

Supplemental Guidance: Recovery is executing information system contingency plan activities to restore organizational 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.

Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24.

4.14   IDENTIFICATION AND AUTHENTICATION

4.14.1 IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to **all personnel**:
   (1) An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
   (2) Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
b. Reviews and updates the current:
   (1) Identification and authentication policy **at least annually**; and
   (2) Identification and authentication procedures **at least annually**.

Supplemental 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. Related control: PM-9.

Control Enhancements: None.
References: FIPS Publication 201; NIST Special Publications 800-12, 800-63, 800-73, 800-76, 800-78, 800-100.

4.14.2 IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates organizational users (or processed acting on behalf of organizational users).

Identification is an act or process that presents an identifier to a system so the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others. Authentication is the act or process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an IS. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees. In addition to identifying and authenticating users at the information system level (i.e., at logon), identification and authentication mechanisms may be employed at the application level, when deemed necessary, to provide increased information security. In general, group accounts are prohibited. Users must be uniquely identified and authenticated, unless an exception has been documented in the SSP and approved by the AO, such as in the case of group accounts.

Supplemental Guidance: Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., 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 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.

In addition to identifying and authenticating users at t h e 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. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.
Reference AC-2 Account Management for further guidance on the use of group accounts

Control Enhancements:
4.14.2.1 IA-2(1) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS *(Removed from DSS Baseline)*

4.14.2.2 IA-2(2) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS *(Removed from DSS Baseline)*

4.14.2.3 IA-2(3) IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS
Control: Information systems shall implement multi-factor authentication for all local access to privileged accounts. Supplemental Guidance: Related control: AC-6.

4.14.2.4   IA-2(4) IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS

Control: Information systems shall implement multi-factor authentication for all local access to non-privileged accounts.

4.14.2.5 IA-2(5) IDENTIFICATION AND AUTHENTICATION | GROUP AUTHENTICATION

Control: The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

Group authentication is discouraged for systems and must be approved by the AO. This control supports insider threat mitigation.

Supplemental Guidance: Requiring individuals to use individual authenticators as a second level of authentication helps organizations to mitigate the risk of using group authenticators.

4.14.2.6 IA-2(8) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS-REPLAY RESISTANT

Control: Information systems shall implement multi-factor authentication and use replay-resistant authentication mechanisms for all network access to privileged accounts. An authentication process is resistant to replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use random or non-repeating values (nonce) or challenges and time synchronous or challenge-response one-time authenticators.

Supplemental 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 nonce or challenges such as TLS and time synchronous or challenge-response one-time authenticators.

4.14.2.7 IA-2(9) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS-REPLAY RESISTANT

Control: The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by recording/replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonce or challenges such as TLS and time synchronous or challenge-response one-time authenticators.

4.14.2.8 IA-2(11) IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS-SEPARATE DEVICE

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 organization-defined strength of mechanism requirements.

Supplemental 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. Related controls: AC-6, AU-2, PE-3, SA-4.

4.14.2.9 IA-2(12) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS *(Removed from DSS Baseline)*

4.14.3 IA-3   DEVICE IDENTIFICATION AND AUTHENTICATION

Control: Information systems shall uniquely identify and authenticate all types of devices before establishing a network connection. This includes, but is not limited to, servers, workstations, printers, routers, firewalls, VoIP telephones, video and VoIP (VVOIP), desktop VTC devices, etc. This control supports insider threat mitigation.

Device identification and authentication provides for unique identification and authentication of devices on a LAN and/or WAN by using, for example, MAC or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses or an organizational authentication solution such as Institute of Electrical and Electronics Engineers (IEEE) 802.1x and Extensible Authentication Protocol (EAP), Remote Authentication Dial In User Service (RADIUS) server with EAP- TLS authentication, or Kerberos.

This control can be tailored out for standalone IS.

Supplemental 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., MAC or TCP/IP addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and EAP, Radius server with EAP-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. Related controls: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.

This includes, but is not limited to servers, workstations, multi-function machines, printers, routers, scanners, firewalls, VoIP telephones, VVOIP, desktop VTC devices, etc.

Control Enhancements:
4.14.3.1 IA-3(1) DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION

Control: The information system authenticates all types of devices before establishing a connection using bidirectional authentication that is cryptographically based. Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk (e.g., remote connections).

Supplemental Guidance: A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that

communicates through a network (e.g., local area or wide area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk (e.g., remote connections). Related controls: SC-8, SC-12, SC-13. NSA-approved or FIPS 140-2 compliant. Reference SC-13. References: None.

4.14.4 IA-4   IDENTIFIER MANAGEMENT

Control: Individual user identifiers (USERIDs) are used for identification of users on information systems, which shall be standardized (e.g., last name first initial, first.lastname) for each system. IA-2 addresses the use of unique identifiers.

The organization manages information system identifiers by:
   a. Receiving authorization from appropriate personnel 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; and
   e. Disabling the identifier after a period not to exceed 90 days of inactivity for individuals, groups, or roles; not appropriate to define for device identifiers; e.g., MAC, IP addresses, or device unique token identifiers.

Supplemental Guidance: Common device identifiers include, for example, MAC, Internet protocol 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.
Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.

Control Enhancements:
4.14.4.1 IA-4(4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS
Control: The organization manages individual identifiers by uniquely identifying each individual as a contractor, government, "civilian, military" and/or foreign nationality as appropriate.

Supplemental Guidance: Characteristics identifying the status of individuals include, for example, foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom organizational personnel are communicating. Related control: AT-2.

4.14.5 IA-5   AUTHENTICATOR MANAGEMENT
Control: 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 within a time period not to exceed 90 days for passwords; system defined time period for other authenticator types;

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 change.

Passwords must meet strong password standards. Examples of situations that may require tailoring include, but are not limited to:

a. The password mechanism does not support strong password requirements;

b. The password is one factor of an authorized, multifactor authentication means; and

c. The password is used by a system process (as opposed to an interactive user session).

Shared (Group) Password [IA-5.a & .j] an account password shared among a group of users (i.e., group account) shall be specifically documented in the SSP and authorized for use by the AO. If specifically authorized, shared account passwords must not knowingly be the same for any other account and shall be changed if a user leaves the group.

Supplemental Guidance: Individual authenticators include, for example, passwords, tokens, biometrics, Public Key Infrastructure (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 one-time 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. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.

Control Enhancements:

4.14.5.1   IA-5(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

Control: The IS for password-based authentication:
  a. Enforces minimum password complexity for IS of at least 14 characters in length for non-privileged accounts and 15 characters in length for privileged accounts; contains a string of characters that does not include the user's account name or full name; includes one or more characters from at least 3 of the following 4 classes: Uppercase, lowercase, numerical & special characters;
  b. Enforces at least a minimum of four changed characters;
  c. Stores and transmits only cryptographically-protected passwords;
  d. Enforces password minimum and maximum lifetime restrictions of at least 1 day lifetime minimum and 90 day lifetime maximum;
  e. Prohibits password reuse for a minimum of 24 password generations; and
  f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

These password requirements are for English display language. Other display languages should use equivalent password strength requirements. Passwords shall not be stored on an information system in clear text. An authorized, non-reversible, encryption algorithm (e.g., hash algorithm) shall be used to transform a password into a format that may be stored in a password file for use during subsequent password-validation. Passwords and password files, when transmitted using electronic means, shall be encrypted using an authorized algorithm.

An approved product vendor's current password hashing algorithm is an authorized algorithm when used on a protected network. When possible, systems shall be configured to automatically notify the user of the requirement to change their password at least fourteen (l4) days before its expiration. The minimum age restriction does not apply to the initial change of a password, help desk password reset, or when compromise of a password is known or suspected.

Supplemental 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.

Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords. Related control: IA-6.

4.14.5.2 IA-5(2) AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION

Control: Information systems that use PKI-based authentication shall;
  a. Validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
  b. Enforce authorized access to the corresponding private key;
  c. Map the authenticated identity to account of the individual or group; and

d.   Implement a local cache of revocation data to support path discovery and validation in cases of inability to access revocation information via the network.

Organizations shall ensure that remote sessions for accessing information systems employ PKI certificates issued by a government-approved registration authority and are audited. If PKI is not feasible, security measures above and beyond standard bulk or session layer encryption shall be implemented (e.g., Secure Shell or VPN with blocking mode enabled) [AC-17(7)].

Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or 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. Related control: IA-6. Control can be tailored out.

4.14.5.3 IA-5(4) AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION

Control: The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy requirements as defined in IA-5(1).

Passwords should be sufficiently strong to resist "password cracking" and other types of attacks intended to discover users' passwords. Information resources should use automated password filters to verify that passwords are created consistent with this document. Automated tools should be accessible to assist users with checking password strengths and generating passwords. A password cracking method shall be used only with written AO authorization providing explicit direction for use during vulnerability testing. Only authorized personnel will have access to and use password cracking tools. Reference IA-5(1) (a) and (b) for password requirements.

Supplemental Guidance: This control enhancement focuses on the creation of strong passwords and the characteristics of such passwords (e.g., complexity) prior to use, the enforcement of which is carried out by organizational information systems in IA-5(1). Related controls: CA-2, CA-7, RA-5.

4.14.5.4 IA-5(7) AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS

Control: The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

Supplemental Guidance: 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).

4.14.5.5 IA-5(8) AUTHENTICATOR MANAGEMENT | MULTIPLE INFORMATION SYSTEM ACCOUNTS

Control: In order to manage the risk of compromise due to individuals having accounts on multiple information systems, the organization implements the following procedures:
   a.   Users cannot use the same password for different systems with domains of differing classification levels;

b.   Users cannot use the same password to access different systems within one class level (e.g., internal agency network and Intelink); and

c.   Users cannot use the same password to access different accounts with different privilege levels (e.g., user, and administrator).

Supplemental Guidance: When individuals have accounts on multiple information systems, there is the risk that the compromise of one account may lead to the compromise of other accounts if individuals use the same authenticators. Possible alternatives include, for example: (i) having different authenticators on all systems; (ii) employing some form of single sign-on mechanism; or (iii) including some form of one-time passwords on all systems.

Organizations define specific requirements for tokens, such as working with a particular PKI.

4.14.5.6 IA-5(11) AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION

Control: The information system, for hardware token-based authentication, employs mechanisms.

Supplemental Guidance: Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government PIV card.

Organizations define specific requirements for tokens, such as working with a particular PKI.

This control can be tailored out.

4.14.5.7 IA-5(13) AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS

Control: The information system prohibits the use of cached authenticators after one hour.

4.14.5.8 IA-5(14) AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES

Control: The organization, for PKI-based authentication, employs a deliberate organization-wide methodology for managing the content of PKI trust stores installed across all platforms including networks, operating systems, browsers, and applications.

4.14.6 IA-6   AUTHENTICATOR FEEDBACK

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

The information systems shall not display any password on a terminal, monitor, or printer. An example of obscuring feedback of authentication information is when a user enters a password and only asterisks are displayed.

Supplemental 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. Related control: PE-18.

Control Enhancements: None. References: None.
4.14.7 IA-7   CRYPTOGRAPHIC MODULE AUTHENTICATION

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. FIPS 140-2 validated cryptographic modules are often used to protect unclassified sensitive information in computer and telecommunication systems (including voice systems). Classified information systems use NSA-validated cryptographic modules.

Supplemental 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. Related controls: SC-12, SC-13.

Control Enhancements: None.
References: FIPS Publication 140; Web: http://csrc.nist.gov/groups/STM/cmvp/index.html.
4.14.8 IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

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

Supplemental 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 non-organizational 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. Related controls: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.

Control Enhancements:
4.14.8.1 IA-8(1) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES

Control: The information system accepts and electronically verifies PIV (e.g., CAC) credentials

Supplemental Guidance: This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). 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 Homeland Security Presidential Directive (HSPD)-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.

4.14.8.2 IA-8(2) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD-PARTY CREDENTIALS

Control: The information system accepts only Federal Identity, Credential, and Access Management (FICAM)-approved third-party credentials.

Third-party credentials are those credentials issued by nonfederal government entities approved by the 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.

Supplemental 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 FICAM Trust Framework Solutions initiative. Related control: AU-2.

4.14.8.3 IA-8(3) IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS

Control: The organization employs only FICAM-approved information system components in Program IS to accept third-party credentials.

Supplemental 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. Related control: SA-4. DoD-approved products shall be used.

Assessment:

4.14.8.4 IA-8(4) IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-ISSUED PROFILES

Control: The IS conforms to FICAM-issued profiles.

Supplemental 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). Related control: SA-4.

Assessment:

4.14.9 IR-1   INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization:
   a. Develops, documents, and disseminates to: organization-defined personnel or roles:
      (1) An incident response policy that addresses purpose, scope, roles, responsibilities,

management commitment, coordination among organizational entities, and compliance;
    (2) Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
  b. Reviews and updates the current:
    (1) Incident response policy **at least annually;** and
    (2) Incident response procedures **at least annually**.

Supplemental 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. Related control: PM-9. Control Enhancements: None. References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.

GCA/Customer is the data owner should contact the GCA/Customer for procedures and guidance with regard to concerns related to the data that resides on the system. If GCA/Customer does not provide procedures/guidance then procedures/guidance contained in this process manual should be followed if the GCA/Customer concurs.

4.14.10 IR-2   INCIDENT RESPONSE TRAINING
Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:
  a. Within **thirty (30) working days** of assuming an incident response role or responsibility;
  b. When required by information system changes; and at least annually thereafter.
  c. Incident recognition and reporting training shall be included as part of both general and privileged user awareness training. See also Security Training [AT-3]. General users must be trained on what constitutes suspicious activity as it applies to the system, other users, and unauthorized individuals internal and external to the organization. General users must also know to whom and when to report suspicious activity and to keep discussions about potential incidents within the incident response chain of command.
  d. Privileged users should be trained in preserving the scene, preserving the data (volatile and nonvolatile), chain of custody, and reporting requirements. Privileged users frequently move from the containment phase to eradication compromising data necessary in prosecuting a potentially criminal case. Privileged users must also know who to contact for assistance in responding to an incident, e.g., the organizations IA point of contact. Additional incident response related training may be required depending on the system, environment, and mission criticality.

Supplemental 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. Related controls: AT-3, CP-3, IR-8.

Control Enhancements:

4.14.11 IR-3   INCIDENT RESPONSE TESTING

Control: The organization tests the incident response capability for the information system at least annually using appropriate tests to determine the incident response effectiveness and documents the results.

Lessons learned should be documented and incorporated into future exercises. If there were no incidents during the past year, the incident response plan shall be tested using a simulated incident/event.

Supplemental 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. Related controls: CP-4, IR-8.

Lessons learned should be documented and incorporated into future exercises. If there were no incidents during the past year, the incident response plan shall be tested using a simulated incident/event.

Control Enhancements:

4.14.11.1   IR-3(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

Control: The organization coordinates incident response testing with organizational elements responsible for related plans.

Supplemental 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. References: NIST Special Publications 800-84, 800-115.

4.14.12 IR-4   INCIDENT HANDLING

Control: Please enter facility specific Incident Response Info. The organization:
   a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery
   b. Coordinates incident handling activities with contingency planning activities and Stakeholders
   c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Supplemental 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 and organizational stakeholders 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). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Individuals involved in incident response, reporting and handling will treat each incident as a potentially criminal case. IA professionals not trained in forensics and investigation should ensure preservation of the scene and contact their IA forensics POC prior to moving from the containment phase to the eradication phase to ensure preservation of data (both volatile and nonvolatile) required for criminal prosecution. The NIST version of the incident response lifecycle is depicted in Figure 3-1 below and described in NIST SP 800-61.

Incidents are identified using the categories below, as indicated in CJSCM 6510.01B, *Cyber Incident handling Program*, Table B-A-2. In addition to selecting the appropriate category, also indicate if the incident resulted in a data spill and/or unauthorized disclosure.

Category	Description
1	**Root Level Intrusion (Incident)-**Unauthorized privileged access to an IS. Privileged access, often referred to as administrative or root access, provides unrestricted access to the IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the IS compromised with malicious code that provides remote interactive control, it will be reported in this category.
2	**User Level Intrusion (Incident)-**Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as user-level access, provides restricted access to the IS based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
3	**Un**successful Activity Attempt (Event)-Deliberate attempts to gain unauthorized access to an IS that are defeated by normal defensive mechanisms. Attacker fails to gain access to the IS (i.e., attacker attempts valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders. Note the above CAT 3 explanation does not cover the "run-of-the-mill" virus that is defeated/deleted by AV software. "Run-of-the-mill" viruses that are defeated/deleted by AV software are not reportable events or incidents and should not be not be annotated in JIMS.

4	**Denial of Service (Incident)-**Activity that denies, degrades or disrupts normal functionality of an IS or DoD information network.
5	**Non-Compliance Activity (Event)-**Activity that potentially exposes IS to increased risk as a result of the action or inaction of authorized users. This includes administrative and user actions such as failure to apply security patches, connections across security domains, installation of Vulnerable applications and other breaches of existing DOD policy.
6	**Reconnaissance (Event)-**Activity that seeks to gather information used to characterize IS, applications, networks, and users that may be useful in formulating an attack. This includes activity such as mapping DOD networks, IS devices and applications, interconnectivity, and their users or reporting structure. This activity does not directly result in a compromise.
7	**Malicious Logic (Incident)-**Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This **only** includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Category 1 or Category 2 incidents, not Category 7. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS.
8	**Investigating (Event)-**Events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing, further review. No event will be closed out as a Category 8. Category 8 will be re-categorized to appropriate Category 1-7 or 9 prior to closure.
9	**Explained Anomaly (Event)-**Suspicious events that after further investigation are determined to be non-malicious activity and do not fit the criteria for any other categories. This includes events such as IS malfunctions and false alarms. When reporting these events, the reason for which it cannot be otherwise categorized must be clearly specified.

The terms used above aid in tracking trends. In rare instances when an incident may need to be reported (reference IR-6) outside. The AO will determine the appropriate category and channel for reporting. An Incident or Reportable Event Category is a collection of events or incidents sharing a common underlying cause for which an incident or event is reported. Each event or incident is associated with one or more categories as part of the incident handling process.
Event 5 Sub-categories:

a. Unmarked IS Components-Unmarked IS components or media that place classified data at risk.
b. Unattended IS Components-Discovery of unlocked active session without user present. c. Unauthorized Software (not malicious)-Software obtained through unofficial channels and installed without proper approval.
c. Other.

Control Enhancements:
4.14.12.1   IR-4(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES
Control: The organization employs automated mechanisms to support the incident handling process. While it is not cost effective for most organizations to maintain an online incident

management system, such as Remedy, there are functions that can be automated to support the incident handling process. For instance mechanisms in support of identification or detection and analysis include:

   a. System audit logs that capture unsuccessful attempts to log into the system, attempts to gain access to unauthorized folders/files, attempts to introduce unauthorized software or media.

   b. Device audit logs.

   c. IDS, content filtering applications, etc.

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

4.14.12.2   IR-4(3) INCIDENT HANDLING | CONTINUITY OF OPERATIONS

Control: The organization identifies classes/categories as defined in CNSS 1002, 1010 to define actions required in the event of an incident to ensure continuation of organizational missions and business functions.

Supplemental Guidance: Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Appropriate incident response actions include, for example, graceful degradation, information system shutdown, fall back to manual mode/alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved solely for when systems are under attack.

A database or spreadsheet may be used to capture information about each incident. This method provides the opportunity to identify the class of each incident to ensure appropriate actions are captured in the updated incident handling procedures.

4.14.12.3   IR-4(4) INCIDENT HANDLING | INFORMATION CORRELATION

Control: The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Supplemental Guidance: Sometimes the nature of a threat event, for example, a hostile cyber-attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by organizations.

Information correlation also provides an automated approach to track trends, i.e., individuals, specific systems, equipment resulting in updated overall training or individual one-on-one recalibration, insight into system or equipment issues that call for closer scrutiny. Including facility and room alarms in the database or spreadsheet can also highlight recurring issues with an alarm on a particular facility or room. Larger corporations should capture all incidents (system and environment) across campus to better assess organization-wide trends, e.g., individuals, equipment. The sum total offers an organization-wide awareness.

4.14.12.4   IR-4(6) INCIDENT HANDLING | INSIDER THREATS-SPECIFIC CAPABILITIES

Control: The organization implements incident handling capability for insider threats.

Supplemental Guidance: While many organizations address insider threat incidents as an inherent part of their organizational incident response capability, this control enhancement provides

additional emphasis on this type of threat and the need for specific incident handling capabilities (as defined within organizations) to provide appropriate and timely responses.

4.14.12.5   IR-4(7) INCIDENT HANDLING | INSIDER THREATS-INTRA-ORGANIZATION COORDINATION

Control: The organization coordinates incident handling capability for insider threats across the Oversight Team.

Supplemental Guidance: Incident handling for insider threat incidents (including preparation, detection and analysis, containment, eradication, and recovery) requires close coordination among a variety of organizational components or elements to be effective. These components or elements include, for example, mission/business owners, information system owners, human resources offices, procurement offices, personnel/physical security offices, operations personnel, and risk executive (function). In addition, organizations may require external support from federal, state, and local law enforcement agencies.

4.14.12.6   IR-4(8) INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS

Control: The organization coordinates with organizations whose data has been involved in an incident to correlate and share incident-related information to achieve a cross-organization perspective on incident awareness and more effective incident responses.

Supplemental Guidance: The coordination of incident information with external organizations including, for example, mission/business partners, military/coalition partners, customers, and multi-tiered developers, can provide significant benefits. Cross-organizational coordination with respect to incident handling can serve as an important risk management capability. This capability allows organizations to leverage critical information from a variety of sources to effectively respond to information security-related incidents potentially affecting the organization's operations, assets, and individuals.

AO notification required prior to notifications to external stakeholders.

4.14.13 IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents.

Collecting user statements of those involved in incidents with information systems is also required in order to completely document the details of an incident. While it is not cost effective for most organizations to maintain an online incident management system, there are functions that can be automated to support the incident handling process. For instance mechanisms in support of identification or detection and analysis include:
   a. System audit logs that capture unsuccessful attempts to log into the system, attempts to gain access to unauthorized folders/files, attempts to introduce unauthorized software or media.
   b. Device audit logs.
   c. IDS, content filtering applications, etc.

Supplemental 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. Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Collecting user statements of those involved in incidents with information systems is also required in order to completely document the details of an incident.

While it is not cost effective for most organizations to maintain an online incident management system, there are functions that can be automated to support the incident handling process. For instance mechanisms in support of identification or detection and analysis include:

  a. System audit logs that capture unsuccessful attempts to log into the system, attempts to gain access to unauthorized folders/files, attempts to introduce unauthorized software or media.
  b. Device audit logs.
  c. IDS, content filtering applications, etc.

4.14.14 IR-6   INCIDENT REPORTING

Control: The organization:

  a. Requires personnel to report suspected security incidents to the organizational incident response capability within 24 hours.
  b. Reports security incident information to **the appropriate DSS representatives (see IR-4(8))**.

In the case of a suspected incident, containment procedures must begin immediately. However, GCA/Confirmation of the classification of the information spilled is required promptly so decisions concerning scale of containment and eradication efforts can be scoped, e.g., data spilled onto another system tends to be (although not always) less critical than data spilled to an unclassified system.

Initial/interim reporting should begin as soon as possible after knowledge of the incident and should continue until the incident is resolved.

Organizations will continue to report until the incident is closed.

Reporting
The facility must make a Preliminary Inquiry immediately to the CSA when there is a loss, compromise, or suspected compromise of classified information, foreign or domestic.

Lead FSO – The originating facility FSO of the contamination leads the effort. The FSO will immediately coordinate and plan the investigation/cleanup considering detailed information such as sender, recipient(s), subject, time sent, day sent, systems and peripherals potentially affected, etc.

If the contractor's preliminary inquiry confirms that a loss, compromise, or suspected compromise of any classified information occurred, the contractor will promptly submit an initial report of the incident unless notified by the CSA. The initial report will be distributed via secure channels (STE, secure fax, cleared network, etc.). If secure channels are not available the initial report will not include location and/or classification of the spill only.

Additionally, the Lead FSO will prepare a final report (NISPOM 1-303c.) when the investigation is completed to the CSA.

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the 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. Related controls: IR-4, IR-5, IR-8.

The ISSM/ISSO must also report the incident to the system AO. Organizations will continue to report until the incident is closed.

Information system-related fraud, waste, and abuse issues should be reported to the organization's chain of command. Individuals also have the right to call the Fraud, Waste and Abuse Center (FWAC) hotline.

Control Enhancements:
4.14.14.1   IR-6(1) INCIDENT REPORTING | AUTOMATED REPORTING
Control: The organization employs automated mechanisms to assist in the reporting of security incidents.

Differing types of automated mechanisms can meet the intent of IR-6(1) This mechanism may be a web-based form that is populated by the ISSM/ISSO alerting the appropriate individuals, or an email process that includes a preset distribution group to ensure all key individuals are alerted in the event of an incident, e.g., ISSM/ISSO, and other designated personnel. Where an email distribution is used, the responder should be cautious unclassified information in the incident description in the initial report. The classified report shall be protected in accordance with the NISPOM requirements.

4.14.14.2   IR-6(2) INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS
Control: ISSM shall report all information system-related incidents to designated personnel providing the response determination, guidance to the site as needed. This provides an organization-wide awareness of incidents, a broader capability for identifying trends and vulnerabilities, and the potential to share information with other organizations in the community. This control supports insider threat mitigation.

ISSM or authorized designated personnel is responsible for reporting incidents external organizations with the potential for harm due to sensitive information being released to outside organizations of perhaps questionable trustworthiness. References: NIST Special Publication 800-61.

4.14.15 IR-7   INCIDENT RESPONSE ASSISTANCE

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 IS for the handling and reporting of security incidents.

Supplemental Guidance: Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. Related controls: AT-2, IR-4, IR-6, IR-8, SA-9.

If the ISSM/ISSO or SA is not trained in incident response and investigation commensurate with the level of skill required for a system, the organization's incident response plan and procedures must reflect reach-back to their POC.

Control Enhancements:
4.14.15.1 IR-7(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT

Control: The organization employs automated mechanisms to increase the availability of incident response-related information and support. Automated mechanisms for incident response related information and support may be employed through a website, database, or other automated means.

Supplemental 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.

Automated mechanisms for incident response related information and support may be employed through a website, database, or other automated means.

4.14.15.2 IR-7(2) INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS

Control: The organization:
   a. Established 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.

The external providers for incident response for IS incidents are the ISSM/ISSOs will provide local incident response team POCs to their POC. The names and contact information may be provided in the SSP. This control supports insider threat mitigation.

Supplemental Guidance: 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.

The external providers for information system protection are the POCs. ISSM/ISSOs will provide local incident response team POCs. The names and contact information may be provided in the SSP. References: None.

4.14.16 IR-8   INCIDENT RESPONSE PLAN

Control: The organization:

Each organization shall develop an incident response plan specific to the system, site, and/or installation as appropriate, which:

   a. Provides a roadmap for implementing its incident response capability.
   b. Describes the structure and organization of the incident response capability.
   c. Provides a high-level approach for how the incident response capability fits into the overall Enterprise.
   d. Meets unique requirements related to mission, size, structure, and functions.
   e. Defines reportable incidents.
   f. Provides metrics for measuring the incident response capability.
   g. Defines the resources and management support needed to effectively maintain and mature the incident response capability.
   h. Is reviewed and approved by the AO.
   i. Identifies how the organization will test (i.e. table-top, hot wash, etc.).

Copies of the incident response plan shall be distributed to all personnel with a role or responsibility for implementing the plan. The incident response plan shall be reviewed at least annually (incorporating lessons learned from past incidents) and revised to address system/organizational changes or problems encountered during plan implementation, execution, or testing. Incident response plan changes shall be communicated to all personnel with a role or responsibility for implementing the plan not later than 30 days after the change is made. The incident response plan shall be protected from unauthorized disclosure and modification.

Supplemental 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. Related controls: MP-2, MP-4, MP-5.

Ensure there is coordination, as appropriate, on the Incident Response Plan and that all incident response personnel who should receive a copy of the plan and any changes are identified by name and/or role.

Control Enhancements: None.
References: NIST Special Publication 800-61.
4.14.17 IR-9   INFORMATION SPILLAGE RESPONSE
Control: The organization responds to information spills by:

   a. Identifying specific information involved in the information system contamination;
   b. Alerting personnel of the information spill using a method of communication not associated with the spill;
   c. Isolating the contamination information system or system component;
   d. Eradicating the information from the contaminated information system or component;
   e. Identifying other IS or system components that may have been subsequently contaminated; and
   f. Performing actions as required by AR 380-381.

Supplemental Guidance: Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to

process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the information system, the specific nature of contaminated storage media, and the access authorizations (e.g., security clearances) of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

DSS-Approved Classified Spill Cleanup Plan

Purpose: This document describes a procedure for cleanup of Information Systems that have been contaminated with classified data. It defines the roles and responsibilities of personnel during incidents such as those caused by inadvertent transmission of classified e-mail over unclassified computer networks and e-mail systems, or by the introduction of data of a higher classification level onto an unaccredited system, or a system accredited at a lower level. The NAO may require additional or alternate cleanup procedures.

Equipment	The process outlined in this document includes both file servers and Exchange servers, laptops/desktops and other systems and peripherals that may have been contaminated with classified information.
Sender/Receiver	This procedure is intended to cover both the computing environment of the sender and receiver(s) of classified e-mails. The initial report of contamination could come from either the sender or receiver. In any event, all potentially contaminated computing environments must be included. In those cases where either the sender or the receiver are not local, the cognizant FSO will make notification to the appropriate security contact at the other known locations where the contamination may exist and include them in the coordination of cleanup actions. Notification of an e-mail spill will NOT be made to any uncleared company or individual that does not fall under the NISPOM (e.g., to a Yahoo user, or to an uncleared company).
Contaminated material	The cognizant FSO will establish the protection for all equipment or material that is believed to be contaminated with classified information. The FSO will determine when an item may be released back into service based on the review of the checklists from the IS team.

Classified Spill Cleanup Procedures

Classified Spills (also known as contaminations or classified message incidents) occur when classified data is introduced to an unclassified computer system or to a system accredited at a lower classification than the data. Any classified spill will involve an Administrative Inquiry (AI) for the facility concerned.

The following procedures apply to all cleared facilities and all contractor systems involved in a classified data spill with information classified Secret and below. Data spills involving TOP SECRET information will be cleaned up following GCA procedures, but at minimum will include these procedures. The focus of cleanup procedures is to identify the degree of the spill, containing it, and cleaning it up.

FSO, ISSMs, ISSOs, system administrators (SAs), etc., are encouraged to become familiar with these procedures prior to an incident. These procedures will be incorporated into the NISPOM training.

Wiping Utility

Hard drives involved in a classified spill should be wiped using an NSA or National Information Assurance Program (NIAP)-approved product, however if one is unavailable any commercially available wiping utility that meets the following requirements may be used:

a.   If wiping whole disks, it must be able to wipe the entire drive (e.g., partition tables, user data, operating systems and boot records).

b.   If wiping whole disks, it must be able to wipe Device Configuration Overlay (DCO) hidden sectors if ATA-6 disks are being used.

c.   If wiping whole disks, it must be able to wipe a Host Protected Area (HPA).

d.   Must be able to sanitize by overwriting with a pattern, and then its complement, and finally with another unclassified pattern (e.g., "00110101" followed by "11001010" and then followed by "10010111" [considered three cycles]). Sanitization is not complete until three cycles are successfully completed.

e.   Must be able to verify the overwrite procedure by randomly re-reading (recommend 10% if possible) from the drive to confirm that only the overwrite character can be recovered. If not, the use of an additional utility to accomplish this is acceptable.

f.   Must be able to print the results of the overwriting operation showing any bad sectors or areas of the disk that could not be written to (if there are any bad sectors or blocks the disk must be destroyed or degaussed).

Cost Analysis

It is suggested that the company perform a cost analysis before using the option of wiping hard drives. Wiping can take many hours to perform and it may be more cost effective to dispose of hard drives by degaussing or destruction. NIST Special Publication 800-88, Guidelines for Media Sanitization can provide some assistance in this regard.

Additional Precautions

The hard drive may not be the only storage media in a system. Beware of floppy disks left in floppy disk drives, Zip disks in Zip drives, CDs and DVDs in optical drives, tapes in tape backup-units, thumb drives/compact flash drives, BIOS passwords, printing devices and the like. Include relevant documentation when an old system is wiped and then transferred from one department or division within the same company to another. Desktops and laptops aren't the only systems that need sanitizing. Pocket PCs, PDAs, some multifunction cell phones, and other devices may also contain sensitive information such as passwords or confidential data.

Coordination Communications – Employees or security managers who report the discovery of classified information on unclassified or lower classified information systems are not to delete the classified data, but to isolate the systems and contact the cognizant FSO, ISSM or ISSO immediately. Caution should be taken when discussing such incidents over unsecured telephones so as not to further endanger any classified information that may be at risk on unclassified systems.

The initial report should include the following (if known):

a.   Origination of data/message: Facility, location, point of contact.

b.   Other facilities involved: Facility, location, point of contact.

   c. Method of transmission.
  d. All equipment involved: Servers (RAID or single), workstations, notebooks, e-mail servers, Blackberries, etc.
  e. Remote dial-in or network connection?
  f. Location of all equipment.
  g. All Operating Systems involved.
  h. Number of people involved (Identify the employee(s) and include clearance level).
  i. Are there backup tapes involved?
  j. Any audit logs available to determine access?
  k. Current status of all equipment involved.
  l. Data owner notified?
  m. Customer information:
   (1) Name;
   (2) Point of Contact;
   (3) Phone numbers; and
   (4) Email address.

A copy of the customer approved clean-up procedures for of all equipment and media

Appropriately Cleared Team
It is essential that all persons who participate in the cleanup have the appropriate clearance/access if they could potentially be exposed to classified information. In cases where the company is a cleared company but without accredited IS and no cleared computer personnel, uncleared personnel will be required to sign a standard non-disclosure agreement.

Protection of classified data and hardware
The cognizant ISSM will interview all appropriate persons to determine the extent of the contamination and to recover any hardcopy or media copies of the classified information. Any contaminated systems such as printers or other peripherals with memory that cannot be readily sanitized will be moved into a controlled area until they can be cleaned. Backup tapes that are determined to contain potential classified material must be identified and secured appropriately until they can be sanitized.

Security Incident Response Procedures
Checklists – The following checklists describe the processes/procedures to sanitize Exchange and GroupWise e-mail servers and e-mail clients. Other e-mail systems must follow comparable processes that comply with the intent of the documented procedures. These standard procedures are to be followed for classification levels of TOP SECRET and below, unless directed by the AO to take more stringent measures.

Transitory Devices
Data that is transmitted through transitory network devices such as mail hubs, routers, etc., is constantly overwritten through normal network operations. Therefore, these sanitization procedures are applicable only to the sending and/or receiving network servers and client workstations.

Control Enhancements:

4.14.17.1   IR-9(1) INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL

Control: The organization assigns personnel and associated roles with responsibility for responding to information spills.

Role	Responsibilities
All Personnel	Immediately communicate to each other any reports of e-mail security incidents or classified contaminations. Participate in and support security incident meetings and response efforts. Assess the risks of the contamination and follow any special guidelines of the data owner (customer). Assign appropriately cleared individuals to participate in the cleanup effort.
FSO	The originating facility FSO of the contamination will act as the incident lead. Notify applicable Government agencies of the security incident. Determine the security classification level of the data and confirm the appropriate cleansing procedures. Identify the sender/receiver(s) of the classified information. Request cleanup assistance by appropriately cleared technicians. Contact the appropriate security official at any distant locations where the contamination was received or from where it originated. Determine if there was "bcc:" addressing or if the sender copied his/her own account. Determine if the contamination was distributed via other paths such as print, ftp, electronic media, server storage, etc. Determine if recipient accounts have user-configured rules for auto-forward, auto-save or other special instructions. Investigate possibility of proxy accounts, Blackberry access, remote access and any other possible "feeds" from the contaminated accounts. Isolate any contaminated assets of the sender/receiver. Notify company officials of the incident and the planned cleanup effort.
ISSM/ISSO	Assess the extent of contamination and plan cleanup actions with the local ISSM. Conduct cleanup of contaminated systems and any peripherals using cleared personnel. Spills at all classification levels will be cleaned up following these procedures at a minimum, but will require GCA approval either prior to (preferable) or after the spill occurs (the GCA may require destruction). If the GCA does not answer within 30 days it will be taken as a concurrence with the procedures and declassification. Report vulnerabilities, cleanup actions and any other pertinent information to local ISSM. Protect and isolate any contaminated systems from further compromise Coordinate storage/transport of classified material or other evidence with the ISSM.

4.14.17.2   IR-9(2) INFORMATION SPILLAGE RESPONSE | TRAINING

Control: The organization provides information spillage response training annually.

4.14.17.3   IR-9(4) INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL

Control: The organization employs security safeguards for personnel exposed to information not within assigned access authorizations, such as making personnel aware of federal laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.

Supplemental Guidance: Security safeguards include, for example, making personnel exposed to spilled information aware of the federal laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.
References: None.

4.14.18 IR-10 INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

Control: The organization establishes an integrated team of forensic/malicious code analysts, tool developers and real time operations personnel.

Supplemental Guidance: Having an integrated team for incident response facilitates information sharing. Such capability allows organizational personnel, including developers, implementers, and operators, to leverage the team knowledge of the threat in order to implement defensive measures that will enable organizations to deter intrusions more effectively. Moreover, it promotes the rapid detection of intrusions, development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated security analysis team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing intelligence development. This enables the team to identify adversary TTPs that are linked to the operations tempo or to specific missions/business functions, and to define responsive actions in a way that does not disrupt the mission/business operations. Ideally, information security analysis teams are distributed within organizations to make the capability more resilient.

Control Enhancements: None. References: None.
4.15   MAINTENANCE

4.15.1 MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization:
   a. Develops, documents, and disseminates to organization-defined personnel or roles:
      (1) A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
      (2) Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
   b. Reviews and updates the current:
      (1) System maintenance policy **at least annually**; and
      (2) System maintenance procedures **at least annually**.

Supplemental 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. Related control: PM-9.

Specific policy and procedures related to system maintenance are defined in the remainder of this section.

Control Enhancements: None.
References: NIST Special Publications 800-12, 800-100.

4.15.2 MA-2   CONTROLLED MAINTENANCE

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 ISSM/ISSO or designee 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 date and time of maintenance, name of individual performing the maintenance, name of escort (if appropriate), a description of the maintenance performed, and a list of equipment removed or replaced to include ID numbers (if applicable) in organization maintenance records or maintenance log.

IS are particularly vulnerable to security threats during maintenance activities. The level of risk is directly associated with the maintenance person's clearance and access status. A maintenance person may be uncleared or may not be cleared to the level of classified information contained on the IS. Properly cleared personnel working in the area must maintain a high level of security awareness at all times during IS maintenance activities. Reference MA-5(1) for escort requirements.

All maintenance activities should be performed on-site whenever possible. Removal of an IS or system components from a facility for maintenance or repairs requires approval coordination with the individual responsible for changes to the system, e.g., ISSM/ISSO and the individual who approves removal of equipment from the facility.

Any maintenance changes that impact the security of the system shall receive a configuration management review and documentation update, as appropriate [MA-2.e]. See also [CM-3].

Organizations shall record all information system repairs and maintenance activity in a maintenance log for the life of the IS and retain the log for a minimum of one year after equipment decommissioning or disposal.

Supplemental 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. Related controls: CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2. References: None.

4.15.3 MA-3   MAINTENANCE TOOLS
Control: The organization approves, controls, and monitors information system maintenance tools. Devices with transmit capability (e.g., IR, RF) shall remain outside the facility unless explicitly approved by the AO.

Supplemental 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. Related controls: MA-2, MA-5, MP-6.

Devices with transmit capability (e.g., IR, RF) shall remain outside the facility unless explicitly approved by the PSO and AO.

Control Enhancements:
4.15.3.1 MA-3(2) MAINTENANCE TOOLS | INSPECT MEDIA
Control: The organization checks media containing diagnostic and test programs for malicious code before the media are used in an IS.

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.

Supplemental 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. Related control: SI-3.

4.15.3.2 MA-3(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL
Control: Organizations are responsible for preventing the unauthorized removal of maintenance equipment from the facility. This can be accomplished by any of the following:
    a.   Verifying there is no organizational information contained on the equipment.

        b.   Sanitizing or destroying the equipment.
   c. Retaining the equipment within the facility.
   d. Obtaining approval from the ISSM/ISSO explicitly authorizing removal of the equipment from the facility.

Media without write protection that is brought in for maintenance must remain within the facility and must be stored and controlled at the classification level of the highest IS to which the media was introduced. Prior to entering the facility, maintenance personnel must be advised that they will not be allowed to remove media from the facility. If deviation from this procedure is required under special circumstances, it must be documented locally for review and approval by the ISSM/ISSO.

Each time the diagnostic test media is introduced into the facility it must undergo stringent integrity checks (e.g., virus scanning, checksum) prior to being used on the IS, and before leaving the facility, the media must be checked to assure that no classified information has been written on it. See also MP-5.

Supplemental Guidance: Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.

Media without write protection that is brought in for maintenance must remain within the facility and must be stored and controlled at the classification level of the highest IS to which the media was introduced. Prior to entering the facility, maintenance personnel must be advised that they will not be allowed to remove media from the facility. If deviation from this procedure is required under special circumstances, it must be documented locally for review and approval by the PSO/GSSO/CPSO and ISSM/ISSO. Each time the diagnostic test media is introduced into the facility it must undergo stringent integrity checks (e.g., virus scanning, checksum) prior to being used on the IS, and before leaving the facility, the media must be checked to assure that no classified information has been written on it. See also MP-5.

The information system restricts the use of maintenance tools to authorized personnel only.

Supplemental Guidance: This control enhancement applies to information systems that are used to carry out maintenance functions. Related controls: AC-2, AC-3, AC-5, AC-6.
References: NIST Special Publication 800-88.

4.15.4 MA-4   NONLOCAL MAINTENANCE
Control: The organization:
   a. Approves and monitors nonlocal maintenance and diagnostic activities;
   b. 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;
   c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; and
   d. Maintains records for nonlocal maintenance and diagnostic activities; and
   e. Terminates session and network connections when nonlocal maintenance is completed.

Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network outside of the system's authorization boundary. Non-local includes devices shipped out for repair or online 'remote' maintenance.

Supplemental 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. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17.

Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network outside of the system's authorization boundary. Non-local includes devices shipped out for repair or online 'remote' maintenance. Access shall be limited to those components of the information system being serviced.

Control Enhancements:
4.15.4.1 MA-4(3) NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION
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.

Supplemental 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. Related controls: MA-3, SA-12, SI-3, SI-7.

If non-local maintenance is required from a service or organization that does not provide the same level of security required for the IS being maintained, the system must be sanitized (see the Media Protection (MP) section) and placed in a standalone configuration prior to establishment of the remote connection. If the system cannot be sanitized (e.g., due to a system crash), non-local maintenance is not permitted.

4.15.4.2 MA-4(6) NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION
Control: The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications. Strong identification and authentication techniques (i.e., two-factor authentication) shall be employed in the establishment of non-local maintenance and diagnostic sessions. Supplemental Guidance: Related controls: SC-8, SC-13.

4.15.4.3   MA-4(7) NONLOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION

The information system implements remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.

Supplemental Guidance: Remote disconnects verification ensures that remote connections from nonlocal maintenance sessions have been terminated and are no longer available for use. Related control: SC-13.

References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15.

4.15.5 MA-5   MAINTENANCE PERSONNEL

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.

If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be employed provided a fully cleared, trained, and technically qualified escort monitors and records their activities in a maintenance log.

Supplemental 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, systems 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. Related controls: AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3.

Control Enhancements:
4.15.5.1 MA-5(1) MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS

Control: The organization:
   a. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens that include the following requirements:
      (1) Maintenance personnel who do not have needed access authorizations, clearances, or access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational

personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

(2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

(3) Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

Supplemental Guidance: This control enhancement denies individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained on organizational information systems. Procedures for the use of maintenance personnel can be documented in security plans for the information systems. Related controls: MP-6, PL-2.

If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be employed provided a fully cleared, trained, and technically qualified escort monitors and records their activities in a maintenance log.

4.16   MEDIA PROTECTION

4.16.1 14.1 MP-1   MEDIA PROTECTION POLICY AND PROCEDURES
Control: The organization:
   a. Develops, documents, and disseminates to **all personnel**:
      (1) A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
      (2) Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
   b. Reviews and updates the current:
      (1) Media protection policy **at least annually**; and
      (2) Media protection procedures **at least annually**.

Supplemental 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. Related control: PM-9.

Government issued media may only be used in the performance of assigned duties; personal use of government issued removable media is prohibited. Personally owned media are prohibited on all information systems.

Page 140

Media which is not write-protected and is placed into an IS must be protected at the highest level of information on the system until reviewed and validated.

Reference CNSS Policy (CNSSP) 26, National Policy on Reducing the Risk of Removable Media for National Security Systems.

Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.
4.16.2 MP-2   MEDIA ACCESS
Control: The organization restricts access to all types of removable digital and non-digital media including, but not limited to, hard disks, floppy disks, zip drives, CDs, DVDs, thumb drives, pen drives, flash drives, and similar USB storage devices.

Where appropriate, all portable media with a moderate or high confidentiality rating shall be encrypted.

All digital media, and the use of such media, must be authorized by the designee, prior to being introduced. Organizations are required to ensure the local facility SOP defines personnel/roles and security measures used to control access to media (i.e. centralized safe, media sign-out logs, media accountability logs, entry/exit procedures, etc.). Maintain a list of authorized users and their respective authorized use privileges. Personally-owned thumb drives, CDs, and DVDs are prohibited from entering accredited facilities without approval.

Supplemental 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. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.

All digital media, and the use of such media, must be authorized by the ISSM, or designee, prior to being introduced into the physical environment Organizations are required to ensure the local facility SOP defines personnel/roles and security measures used to control access to media (i.e. centralized safe, media sign-out logs, media accountability logs, entry/exit procedures, etc.).

Maintain a list of authorized users and their respective authorized use privileges.

Personally-owned thumb drives, CDs, and DVDs are prohibited from use on classified systems

Control Enhancements:
4.16.3 MP-3   MEDIA MARKING
Control: The organization:
   a. Marks IS media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information
   b. Exempts new, unused, factory-sealed media from marking as long as the media remains

within the locked media cabinet or storage area.

All information storage media must be appropriately marked and protected to prevent the loss of information through poor security procedures. Likewise, to prevent security compromises, all output products (to include printed material) must be appropriately marked and protected. Each user is ultimately responsible for the marking, handling, and storage of media and paper products within their assigned area of responsibility. In addition, security markings will be displayed on all servers, server cabinets, desktops/laptops, removable/external hard drives, monitors and printers. Thin clients must also be marked. In the case of multi-level devices the security marking shall reflect the highest classification level authorized to be processed.

All IS storage media shall have external security markings clearly indicating the classification of the information. All information storage media will be marked. [MP-3(a)] See the NISPOM for additional media marking information.

Supplemental 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. Related controls: AC-16, PL-2, RA-3.

Note that NIST makes a distinction between 'security marking' and 'security labeling' as indicated in the supplemental guidance above. All media will be marked in accordance NISPOM.

All information storage media must be appropriately marked and protected to prevent the loss of information through poor security procedures. Likewise, to prevent security compromises, all output products (to include printed material) must be appropriately marked and protected. Each user is ultimately responsible for the marking, handling, and storage of media and paper products within their assigned area of responsibility.

In addition, security markings will be displayed on all servers, server cabinets, desktops/laptops, removable/external hard drives, monitors and printers. Thin clients must be marked to the highest classification level authorized to be processed.

Additionally, media labels shall not cover the serial number of the device or account control numbers. Labels made specifically for CD/DVDs may be applied directly to CD/DVDs. All required information may also be written on the media with a paint-pen, media label maker or permanent marker.

Control Enhancements: None. References: FIPS Publication 199.

4.16.4 MP-4   MEDIA STORAGE

Control: The organization:

a. Physically controls and securely stores all digital media regardless of classification and/or non-digital media containing classified information within an area and/or contained approved for processing and storing media based on the classification of the information contained within the media; and

b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Commercial software maintained within the facility by IT personnel and used to update systems or maintain proof of license or purchase may be handled separately from the facility tracking log or system. This media must be locked away in a separate container or cabinet and treated as unclassified provided the write protection or verification of closed session was verified by IT personnel once it was used in a classified computer system. Commercial media still in shrink-wrap may remain this way and be secured in the same cabinet as other commercial media.

All media shall be accounted for under the direct management of the Top Secret Control Officer (TSCO) in accordance with the NISPOM, section 5-201.

Supplemental 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 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. Related controls: CP-6, CP-9, MP-2, MP-7, PE-3.

Control Enhancements:

4.16.5 MP-5   MEDIA TRANSPORT

Control: The organization:

a. Protects and controls all types of digital and non-digital media during transport outside of controlled areas using AO approved security measures, to include courier and digital media encryption;

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. Transport of media shall be restricted to an authorized custodian by means of a courier card\letter.

Approved procedures shall be implemented to address mobile devices traveling to and returning from a location that the organization deems to be of significant risk. Information should be

transported electronically whenever possible. When electronic transport is not possible, movement of all media shall be coordinated through the appropriate security personnel (ISSM/ISSO.) following approved procedures. [MP-5(a)]

Activities associated with the transport of media shall be documented by the organization. Appropriate entries in the organization's media accounting system shall be made. [MP-5(b)]

Supplemental 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. Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.

Control Enhancements:
4.16.5.1 MP-5(3) MEDIA TRANSPORT | CUSTODIANS
Control: The organization employs an identified custodian during transport of information system media outside of controlled areas. Transport of media shall be restricted to an authorized custodian by means of a courier card/letter.

Supplemental Guidance: Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

Transport of media shall be restricted to an authorized custodian by means of a courier card/letter.

4,16.5.2 MP-5(4) MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION
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. 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). Cryptographic mechanisms during transport outside of controlled areas shall be either NSA-approved or FIPS 140-2 compliant.

Supplemental 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). Related control: MP-2.

Cryptographic mechanisms during transport outside of controlled areas shall be either NSA-approved or FIPS 140-2 compliant. References: FIPS Publication 199; NIST Special Publication 800-60.

4.16.6 MP-6   MEDIA SANITIZATION

Control: See the DAAPM, MP-6, for additional sanitization requirements for specific types of media.

The organization:
   a. Sanitizes all digital and non-digital media prior to disposal, release out of organizational control, or release for reuse using in accordance with **NSA/CSS PM 9-12** 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.

Supplemental 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. Related controls: MA-2, MA-4, RA-3, SC-4.

In addition to NSA/CSS Policy Manual 9-12, Storage Device Sanitization Manual (SDDM), also reference the most current NSA/CSS Degausser Evaluated Products List (EPL) and other NSA references located on NSA's Media Destruction Guidance website:
https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

Before storage media is released out of organizational control, becomes obsolete, or is no longer usable or required for an information system, it is a requirement to ensure that residual magnetic, optical, electrical, or other representations of data which have been deleted are no recoverable.

Sanitization is the process of removing information from storage devices or equipment such that data recovery using any known technique or analysis is prevented. Sanitization includes the removal of data from the storage device, as well as the removal of all labels, markings, and activity logs.

Destruction is the process of physically damaging media so that it is not usable and there is no known method of retrieving the data. This may include degaussing, incineration, shredding, grinding, embossing, chemical immersion, etc.

All sanitization and destruction procedures require AO approval, and must be in accordance with the current version of the NSA/CSS Policy Manual 9-12. Organizations may also institute additional media sanitization policies and procedures as needed.

Responsibilities
Organizations are responsible for ensuring adequate resources and equipment are available to support media sanitization activities.

The ISSM is responsible for the security of all media assigned to the organization and under his/her purview. To protect these assets, he/she must ensure the security measures and policies contained within this section are followed. Additionally, the ISSM, with AO approval, may publish supplemental organizational procedures (SOPs, etc.) for sanitizing, and releasing system memory or media.

Ensure appropriate safeguards are in place so removable media that contain classified, sensitive, or controlled unclassified information are properly sanitized, destroyed, and/or disposed of in accordance with an approved method when no longer needed.

Sanitization of Media
Prior to media disposal, release out of organizational control, or release for reuse, organizations will sanitize all media using sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

All media, regardless of classification, shall be sanitized in accordance with Policy Manual 9-12 prior to release, or disposal. Media may be reused at the same level (classification, category, and caveat) without sanitization.

Degaussing Magnetic Media
Degaussers are ineffective in erasing optical and solid state storage devices.

Degaussing (i.e., demagnetizing) is a method of sanitization. Degaussing is a procedure that reduces the magnetic flux on media virtually to zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is not an approved method for sanitizing optical media.

It is highly recommended that after degaussing, but prior to disposal, all media is physically damaged to prevent data recovery attempts.

Refer to the NSA's website for media destruction guidance including the current *Evaluated Products List – Degausser*. This EPL specifies the model identification of current equipment units that were evaluated against and found to satisfy the requirements for erasure of magnetic storage devices that retain sensitive or classified data.

Sanitizing Optical Media (Destruction)
Optical storage devices include CDs and DVDs. Optical storage devices cannot be sanitized, only destroyed. Refer to Policy Manual 9-12 for detailed procedures related to the sanitization of optical media. Equipment approved for use in the destruction of optical media can be found in the NSA/CSS Evaluated Products List for Optical Media Destruction Devices.

Sanitizing Solid State Storage Devices (Destruction)
Solid state storage devices include Random Access Memory (RAM), Read Only Memory (ROM), Field Programmable Gate Array (FPGA), smart cards, and flash memory. Refer to Policy Manual 9-12 for detailed procedures related to the destruction (e.g., smelting) of solid state storage devices.

Release of Systems and Components
The ISSM/ISSO, in conjunction with the organization's equipment custodian shall develop equipment removal procedures for systems and components as approved by the AO. When such equipment is no longer needed, it can be released if:
   a. It is inspected by the ISSM/ISSO. This inspection will assure that all media, including all internal disks and nonvolatile memory components and boards, have been removed or sanitized.
   b. A record is created of the equipment release indicating the procedure used for sanitization and date of release to the equipment custodian. The record of release shall be retained by the ISSM/ISSO for a period of two years.

Release of Memory Components and Boards
A memory component is considered to be the Lowest Replaceable Unit (LRU) in a hardware device. Memory components reside on boards, modules, and subassemblies. A board can be a module, or may consist of several modules and subassemblies. Memory components are specifically handled as either volatile or nonvolatile, as described below.

Volatile Memory Components
Memory components that **do not** retain data after removal of all electrical power sources, and when reinserted into a similarly configured system, are considered volatile memory components. Volatile components that have contained extremely sensitive or classified information may be released only in accordance with Policy Manual 9-12.

Nonvolatile Memory Components
Components that **do** retain data when all power sources are discontinued are nonvolatile memory components. Some nonvolatile memory components (e.g., ROM, Programmable ROM (PROM), or Erasable PROM (EPROM)) and their variants that have been programmed at the vendor's commercial manufacturing facility and are considered to be unalterable in the field may be released. When in doubt, assume the component can be altered. All other nonvolatile components

(e.g., removable/non-removable hard disks) may be released after successful completion of the sanitization procedures as defined in Policy Manual 9-12.

Other Nonvolatile Media
The following nonvolatile media could possibly retain data when all power sources are discontinued.

a. **Visual Displays.** There are many types of video display technologies in use. These technologies are susceptible, to differing degrees, to a phenomenon called "burn-in". Burn-in occurs when the normally volatile components of the display mechanism becomes worn or damaged and retain evidence of the data they were displaying. A visual display may be considered sanitized if no sensitive or classified information is remains in the visual display. If this information is visible on any part of the visual display face, the display shall be sanitized before it is released from control.

The display technology in common use is liquid crystal display (LCD). When powered for a long period in the rotated position a liquid crystal may retain some of its twist and will not relax to its normal orientation. This is referred to as burn-in even though it is physically twist-in. This burn-in is not typically a problem for LCD displays that do not display an image for days on end. If LCD burn-in is suspected, the ISSO/SA shall uniformly illuminate each pixel of the display then visually search for contrasting areas that reveal information. Vary the intensity across the range of off to saturation for each color (red, green, and blue).

LCDs with compromising burn-in areas identified during assessment can normally be sanitized by leaving the device off for a few days in a warm (<140 degrees Fahrenheit) environment until the liquid crystals relax. If this insufficient then the display should be alternated between long periods of full white and full black until the liquid crystals relax. If all this is insufficient or the display is strongly suspect, then the liquid crystal medium in the offending area of the display between the front and rear LCD plates must be disturbed or removed. The liquid crystal medium is non-toxic but messy.

Actual burn-in can occur in legacy cathode ray tube, plasma, and laser phosphor displays. Where bright images are displayed for long period of time in the same location, the screen phosphors overheats and the image is permanently burned-in. The ISSO/SA shall inspect the face of the visual display without power applied. If sensitive information is visible (typically as a dark spot), the visual display shall be sanitized before releasing it from control. If nothing is visible, the ISSO/SA shall apply power to the visual display; then vary the intensity from low to high.

In accordance with NSA/CSS Policy Manual 9-12, CRT, plasma, and laser phosphor displays visual displays exhibiting burn-in shall be sanitized by destroying the display surface of the monitor into pieces no larger than five centimeters square. Be aware of the hazards associated with physical destruction of monitors.

LED displays (not LCDs with LED illumination) use an LED per pixel color and may have burn-in when LEDs overheat and fail. LED displays are typically used in signage and not on desktop displays. Destruction shall be sufficient to preclude the derivation of sensitive or classified information from the arrangement of the inoperative LEDs.

a. **Printer Platens and Ribbons.** Printer platens and ribbons shall be removed from all printers before the equipment is released. One-time ribbons and inked ribbons shall be destroyed as sensitive material. The rubber surface of platens shall be sanitized by wiping the surface with alcohol.

(1) Laser Printer Drums, Belts, and Cartridges.

(2) Laser printer components containing light-sensitive elements (e.g., drums, belts, and complete cartridges) shall be sanitized before release from control.

(3) Used toner cartridges from properly operating equipment that has completed a full printing cycle (without interruption) may be treated, handled, stored and disposed of as unclassified and may be recycled. When a laser printer does not complete a printing cycle (e.g., a paper jam or power failure occurs), the toner cartridge may NOT be treated as unclassified. If the toner cartridge is removed without completing a print cycle, the cartridge drum must be inspected by lifting the protective flap and viewing the exposed portion of the drum. If residual toner is present, manually rotating the drum is sufficient to wipe off residual toner material present. Alternatively, a subsequent print cycle may be completed and is sufficient to wipe residual toner from the cartridge drum. After completing sanitization actions, the toner cartridge may be treated, handled, stored, and disposed of as unclassified (to include recycling).

b. **Multifunction Devices.** Multifunction devices, including digital copiers and copier or printer centers, have the capability to copy, print, scan, and fax, either in a standalone mode or networked. These devices are computer-based, network-capable devices with processors, memory, hard drives, image retention components, and, in some cases, cellular phone transmitters with vendor auto-alert features. When using multifunctional printer/copier equipment, the document image may remain on the imaging drum/belt, hard drives, and static RAM. All memory resident components of multifunction devices must be properly sanitized before release.

Destroying Media

Follow guidelines established in NSA/CSS Policy Manual 9-12. Media and memory components that are damaged, malfunction, or become unusable must be destroyed using methods appropriate for the media type.

Control Enhancements:

4.16.6.1 MP-6(1) MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT/VERIFY

Control: The organization reviews, approves, tracks, documents and verifies media sanitization and disposal actions.

Supplemental 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. Related control: SI-12.

4.16.6.2 MP-6(2) MEDIA SANITIZATION | EQUIPMENT TESTING

Control: The organization tests sanitization equipment and procedures at least annually to verify that the intended sanitization is being achieved.

Supplemental 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).

Note that NSA/CSS Degausser Evaluated Products List, dated February 1, 2015, and subject to frequent updates states: "…customers should have their equipment re-tested periodically according to the manufacturer's recommendations."

Example: Data Security, Inc. currently recommends that their degaussers be tested (aka certified) every six months for the first two years of operation and then annually thereafter. Testing may be accomplished using the Field CheckR, which requires the user to maintain a log of the test results; or using a certified tape, which is returned to the vendor, in this case Data Security, Inc. for results.

4.16.6.3 MP-6(3) MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES

Control: The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the IS. The use of nondestructive sanitization techniques (e.g., not destroying the hard drive) are for initial sanitization of media prior to first use and not when the contents of the digital media require retention.

Supplemental Guidance: This control enhancement applies to digital media containing classified information and Controlled Unclassified Information (CUI). Portable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information systems through USB ports or other entry portals. While scanning such storage devices is always recommended, sanitization provides additional assurance that the devices are free of malicious code to include code capable of initiating zero-day attacks.

Organizations consider nondestructive sanitization of portable storage devices when such devices are first purchased from the manufacturer or vendor prior to initial use or when organizations lose a positive chain of custody for the devices. Related control: SI-3.

The use of nondestructive sanitization techniques (e.g., not destroying the hard drive) are for initial sanitization of media prior to first use and not when the contents of the digital media require retention.

4.16.7 MP-7   MEDIA USE

Control: Using technical safeguards, the organization prohibits the use of certain types of media on IS; e.g., restricting the use of flash drives or external hard disk drives without the authorization of the AO.

Media Reuse

Certain types of electronic media that have been previously classified under one program may be reused by another program of the same classification level or higher (e.g., S//ABC hard disk is transferred to S//XYZ, or S//ABC hard disk is transferred to TS//LMNO). The individual types of media required for reuse must have specific procedures documented and approved by the system AO. Best practices for wiping magnetic media or SSD for reuse include:

     a. One time overwrite utilizing a known pattern and an AO approved product, and then verifying that the overwrite was successful utilizing a hex editor tool from the first to last sector; or

     b. Encrypt the whole media with an AO approved whole disk encryption (WDE) tool and then destroy the key.

Page 150

For any media type the spirit of the procedures must ensure any labels or evidence of the previous program has been removed prior to handoff to the gaining ISSM or Security Officer.

Least Privilege [AC-6] and Separation of Duties [AC-5] are related controls and should be enforced to the maximum extent possible to prevent unauthorized removal of information from the system.

Supplemental 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. Related controls: AC-19, PL-4.

Media use must be controlled at the end point as technically implemented in AC-6(1).

Media Reuse
Certain types of electronic media that have been previously classified under one program may be reused by another program of the same classification level or higher (e.g., S//ABC hard disk is transferred to S//XYZ, or S//ABC hard disk is transferred to TS//LMNO). The individual types of media required for reuse must have specific procedures documented and approved by the system AO. Best practices for wiping magnetic media or SSD for reuse include: 1. One time overwrite utilizing a known pattern and an AO approved product, and then verifying that the overwrite was successful utilizing a hex editor tool from the first to last sector; or 2. Encrypt the whole media with an AO approved whole disk encryption (WDE) tool and then destroy the key. For any media type the spirit of the procedures must ensure any labels or evidence of the previous program has been removed prior to handoff to the gaining ISSM or Security Officer.

Least Privilege [AC-6] and Separation of Duties [AC-5] are related controls and should be enforced to the maximum extent possible to prevent unauthorized removal of information from the system.

Control Enhancements:
4.16.7.1 MP-7(1) MEDIA USE | PROHIBIT USE WITHOUT OWNER
Control: The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Supplemental 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). Related control: PL-4.

4.16.8 MP-8   MEDIA DOWNGRADING

Control: The organization:
   a. Establishes a media downgrading process that includes employing downgrading mechanisms based on the classification of the media;
   b. Ensures that the IS media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;
   c. Identifies the IS media requiring downgrading; and
   d. Downgrades the identified IS media using the established process.

Supplemental Guidance: This control applies to all information system media, digital and non-digital, subject to release outside of the organization, whether or not the media is considered removable. The downgrading process, when applied to system media, removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading of media also ensures that empty space on the media (e.g., slack space within files) is devoid of information.

Control Enhancements:
4.16.8.1 MP-8(1) MEDIA DOWNGRADING |DOCUMENTATION OF PROCESS
Control: The organization documents information systems media downgrading actions.
The Organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Supplemental Guidance: Organizations can document the media downgrading process by providing information such as the downgrading technique employed, the identification number of the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action.

4.16.8.2 MP-8(2) MEDIA DOWNGRADING |EQUIPMENT TESTING
Control: The organization employs appropriate tests of downgrading equipment and procedures to verify correct performance at least annually.

4.16.8.3 MP-8(4) MEDIA DOWNGRADING |CLASSIFIED INFORMATION
Control: The organization downgrades IS media containing classified information prior to release to individuals without required access authorizations in accordance with NSA standards and policies. This control may only need to be addressed if a system downgrade or tech transfer is required, e.g., based on an authorized administrative information downgrade (classification/program levels) by an Original Classification Authority (OCA).

Supplemental Guidance: Downgrading of classified information uses approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified information systems to unclassified media.

This control may only need to be addressed if a system downgrade or tech transfer is required, e.g., based on an authorized administrative information downgrade (classification/program levels) by an OCA. References: None.

4.17 PHYSICAL AND ENVIRONMENTAL PROTECTION

This section comprises the physical and environmental protections for the DoD SAP Community and for all information systems under the purview of the CA SAPCOs as they relate to physical and environmental protection.

4.17.1 PE-1   PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization:
   a. Develops, documents, and disseminates to **all 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 the current:
      (1) Physical and environmental protection policy **at least annually**; and
      (2) Physical and environmental protection procedures **at least annually**.

Supplemental 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. Related control: PM-9.

Control Enhancements: None.
References: NIST Special Publications 800-12, 800-100;
4.17.2 PE-2   PHYSICAL ACCESS AUTHORIZATIONS
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 [annually or as policy and procedures dictate changes are required]; and
   d. Removes individuals from the facility access list when access is no longer required.

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. This control only applies to areas within facilities that have not been designated as publicly accessible. Ensure Support Systems are controlled within and managed by cleared individuals. Support Systems include card/badge creation systems, card reader systems,

alarm systems, and music sound cover systems. These systems may be addressed in the Fixed Facility Checklist (FFC) or Facility SOP.

Supplemental 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. Related controls: PE-3, PE-4, PS-3.

Ensure Support Systems are controlled and managed by cleared individuals. Support Systems include card/badge creation systems, card reader systems, alarm systems, and music sound cover systems.

Control Enhancements:
4.17.2.1 PE-2(3) PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS
Control: The organization restricts unescorted access to the facility where the information system resides to personnel with security clearances and/or formal access approval as defined by the local security policy (i.e., Facility SOP).

Supplemental Guidance: Due to the highly sensitive nature of classified information stored within certain facilities, it is important that individuals lacking sufficient security clearances, access approvals, or need to know, be escorted by individuals with appropriate credentials to ensure that such information is not exposed or otherwise compromised. Related controls: PS-2, PS-6.

Consider tailoring in PE-5(2) for an environment where not everyone has formal access to all information to restrict access to printer output. Also consider tailoring in PE-6(2) for multi-system server rooms. References: None.

4.17.3 PE-3   PHYSICAL ACCESS CONTROL
Control: The organization:
   a. Enforces physical access authorizations by: Verifying individual access authorizations before granting access to the facility; and Controlling ingress/egress to the facility;
   b. Maintains physical access audit logs;
   c. Provides security safeguards to control access to areas within the facility officially designated as publicly accessible. Physical casings include for example, locking computer racks to protect mission critical servers, network routers, etc. As an alternative, these devices may be secured in a room (e.g., a server room) with access limited to privileged users;
   d. Escorts visitors and monitors visitor activity;
   e. Secures keys, combinations, and other physical access devices;
   f. Inventories physical access devices within as required; and
   g. Changes combinations and keys when first installed or used; if believed to have been subjected to compromise; and when considered necessary by the cognizant security authority (CSA) and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Supplemental 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. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.

Physical casings include for example, locking computer racks to protect mission critical servers, network routers, etc. As an alternative, these devices may be secured in a room (e.g., a server room) with access limited to privileged users.

Control Enhancements:
4.17.3.1 PE-3(1) PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS
Control: The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility for those areas where there is a concentration of IS components (e.g., server rooms, media storage areas, etc.)

Supplemental Guidance: This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers). Related control: PS-2.

**4.17.3.2 PE-3(2) PHYSICAL ACCESS CONTROL | FACILITY / INFORMATION
      SYSTEM BOUNDARIES**
Control: The organization performs random security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or removal of information system components.

Supplemental Guidance: Organizations determine the extent, frequency, and/or randomness of security checks to adequately mitigate risk associated with exfiltration. Related controls: AC-4, SC-7.

4.17.3.3   PE-3(3) PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS / ALARMS / MONITORING

Control: The organization employs guards and/or alarms to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.
Supplemental Guidance: Related controls: CP-6, CP-7.

4.17.4 PE-4   ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities. Security safeguards include locked wiring closets, disconnected or locked spare jacks, and protection of cabling by conduit or cable trays.

Supplemental 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. Related controls: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8.

Control Enhancements: None. References: NSTISSI No. 7003.
4.17.5 PE-5   ACCESS CONTROL FOR OUTPUT DEVICES

Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Supplemental 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. Related controls: PE-2, PE-3, PE-4, PE-18.

Keyboard/Video/Mouse Switch Usage
The application of multi-use or KVM switches provides substantial benefits, in cost reduction, space utilization, and operations enhancement when properly procured, installed, configured, and managed. The introduction and use of these devices in a classified environment, however, presents a moderate degree of risk to classified or sensitive information and systems.

To minimize the risk of inadvertently entering information onto the wrong network, the following requirements shall be satisfied when using KVM switches in Closed Areas:
  a. KVM switches shall be authorized via approved configuration control processes and be annotated in the appropriate system documentation.
  b. The ISSM shall approve the connection of any information system to a KVM switch. When connecting a KVM switch to systems/networks with multiple AOs, each AO's approval shall be obtained prior to installation. Best practice dictates that a KVM switch used across classifications or security boundaries should conform to the NIAP approved Protection Profiles (PP) for peripheral sharing switches and be identified on the NIAP Product Compliant List (PCL) or the NIAP Validated Products List (VPL). Products that have been moved to the NIAP Archived Products List may continue to be used if already deployed within an organization's IT infrastructure.
  c. KVM switches shall be installed in facilities approved for operation of the highest classification information system by authorized SAs or maintenance personnel.

      d.   USB keyboard/mouse connections must only allow Human Interface Device (HID) type (i.e., manual operation) connections. Systems using KVM switches shall not use keyboards or mice with wireless technology.

    e. Positive and deliberate operator action is required to switch between connected systems; switches that automatically scan and switch between systems are not authorized; hot key switching capability is only authorized when all connected systems operate at the same classification level and accesses. Note: A KVM switch between components of the same system (e.g., between a file server and a mail server) need not be certified unless otherwise indicated by the CTTA.

    f. Systems using KVM switches shall not employ "smart" or memory enhanced/data retaining keyboards, monitors or mice. These types of interfaces provide memory retention that creates a risk of data transfer between systems of different classifications.

    g. Systems joined by multi-position switches shall utilize desktop backgrounds or banner software that display classification banners at the top and bottom. The classification banner will state the overall classification for the system in large bold type, and the banner background will be in a solid color that matches the classification (e.g., TS//SCI-yellow, Top Secret-orange, Secret-red, Confidential-blue, Unclassified-green). When systems have a similar classification level (e.g., SECRET and SECRET//NOFORN), but require separation for accessibility, releasability or other constraints, use of unique colors for the different systems is allowed.

    h. Screen lock applications shall display the maximum classification of the system currently logged into and shall require the user to re-authenticate to unlock the screen.

    i. Data of a higher classification shall not be introduced into a system of a lower classification.

    j. The use of switchboxes for print services between classification and compartment levels is prohibited. Switchboxes may be used between the same classification and compartment levels for print services.

    k. Users shall ensure different/unique passwords are used for each system connected through a multi-position switch.

    l. ISSM/ISSO/Supervisors shall ensure user training and compliance to the requirements associated with the introduction and use of multi-position switches.

Keyboard/Video/Mouse Switch Configuration
All KVM switch positions, cables, and connectors shall be clearly marked with the appropriate classification labels and corresponding color. Refer to Figure 3-2, SF 700 Series Labels.

The ISSM/ISSO is responsible for ensuring consistent port order and identification of all KVM switches within the Closed Areas. Where possible, a blank port shall be used between unclassified and classified networks. In addition, if multiple ports are unused, blank ports shall be placed between classification levels whenever possible. There is no requirement to apply tamper-resistant tape or other physical mechanisms to KVM switches.

4.17.5.1 PE-5(3) ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES
Control: The organization marks all output devices in facilities containing information systems that store, process or transmit classified information indicating the appropriate security marking of the information permitted to be output from the device.

Supplemental Guidance: Outputs devices include, for example, printers, monitors, facsimile machines, scanners, copiers, and audio devices. This control enhancement is generally applicable to information system output devices other than mobiles devices.

If Foreign Nationals are located in a facility, output devices of US-only systems must be under constant observation by cleared US personnel. References: None.

4.17.6 PE-6   MONITORING PHYSICAL ACCESS
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 at least every 90 days or as required upon occurrence of physical access incidents; and
   c. Coordinates results of reviews and investigations with the organizational incident response capability.

Supplemental 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. Related controls: CA-7, IR-4, IR-8.

Control Enhancements:
4.17.6.1 PE-6(1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT
The organization monitors physical intrusion alarms and surveillance equipment.

4.17.7 PE-8   VISITOR ACCESS RECORDS
Control: The organization:
   a. Maintains visitor access records to the facility where the information system resides for the period required by NISPOM (at least 2 years).
   b. Reviews visitor access records at least every 90 days.

Supplemental 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.

Control Enhancements:
4.17.8 PE-12   EMERGENCY LIGHTING
Control: The organization employs and maintains automatic emergency lighting for the IS that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Related controls: CP-2, CP-7.

4.17.9 PE-13   FIRE PROTECTION

Control: The organization employs and maintains fire suppression and detection devices/systems for the IS that are supported by an independent energy source.

As described in DoD Manual (DoDM) 5205.07-V3 fire detection systems shall not be tied into the facility's IDS. The fire suppression and detection devices/systems, with the exception of tactical environments, shall activate automatically and notify the organization and emergency responders in the event of a fire. Automatic fire suppression capability is required when the facility is not staffed on a continuous basis.

Additionally, organizations shall ensure the facility undergoes, in accordance with local regulations, fire marshal inspections and promptly resolves identified deficiencies.

Supplemental 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. Fire detection systems shall not be tied into the facility's IDS.

4.17.10 PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: Organizations shall maintain temperature and humidity levels within the facility where the information systems reside at acceptable levels, as defined by the organization, and shall continuously monitor these levels. In addition, organizations shall ensure that temperature and humidity controls with remote maintenance and testing (RMAT) capability are properly configured for use by disabling automatic or remote connection capability. When remote connection capability is required for central management of the HVAC system, it shall be identified on the FFC and approved by the CSA.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms. Related control: AT-3.

Organizations shall ensure that temperature and humidity controls with RMAT capability are properly configured for use in a facility by disabling automatic or remote connection capability. When remote connection capability is required for central management of the HVAC system, it shall be identified on the FFC and approved by the CSA.

4.17.11 PE-15 WATER DAMAGE PROTECTION

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

This control applies primarily to facilities containing concentrations of IS resources; for example, server rooms, data centers, etc.

Supplemental 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. Related control: AT-3.

4.17.12 PE-16 DELIVERY AND REMOVAL

Control: The organization authorizes, monitors, and controls all IS components entering and exiting the facility and maintains records of those items.

Supplemental 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. Related controls: CM-3, MA-2, MA-3, MP-5, SA-12.

Control Enhancements: None. References: None.

4.17.13 PE-17 ALTERNATE WORK SITE

Control: The organization employs management, operational and technical information system security controls at the alternate work site equivalent to those applicable to the primary work site. These security controls shall be assessed as feasible to determine the effectiveness of these controls. The alternate work site shall provide a means for employees to communicate with information security personnel in case of security incidents or problems.

Supplemental 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. Related controls: AC-17, CP-7.

This control is likely to be tailored out if the system availability impact level is low and alternate work sites are not required for the system.

Control Enhancements: None. References: NIST Special Publication 800-46.

4.17.14 PE-19 INFORMATION LEAKAGE

Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.

Information systems, peripherals, associated data communications, and networks (planned or installed) that may be used to process national security or security-related information may need to meet certain national TEMPEST policies and procedures. The objective is to minimize the risk of Foreign Intelligence Services (FIS) exploiting unintentional emanations from intelligence systems. TEMPEST is a short name referring to investigations and studies of compromising emanations. Please refer to CNSSI 7003.

Supplemental Guidance: Information leakage is the intentional or unintentional release of information to an untrusted environment from electromagnetic signals emanations. Security categories or classifications of information systems (with respect to confidentiality) and organizational security policies guide the selection of security controls employed to protect systems against information leakage due to electromagnetic signals emanations.

Control Enhancements:

4.17.14.1   PE-19(1) INFORMATION LEAKAGE | NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES

Control: The organization ensures that IS component, associate data communications, and networks are protected in accordance with national emissions and TEMPEST policies and procedures based on the security category or classification of the information.

In accordance with NISPOM Chapter 11-101, TEMPEST requirements are imposed by contract References: FIPS Publication 199. References: None.

4.18   PLANNING

4.18.1 PL-1   SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization:
   a. Develops, documents, and disseminates to **[all 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;
   b. Reviews and updates the current:
      (1) Security planning policy **[annually]**; and
      (2) Security planning procedures **[annually]**.

Supplemental 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. Related control: PM-9.

Specific policy and procedures related to planning are defined in the remainder of this section.

Control Enhancements: None. References: NIST Special Publications 800-12, 800-18, 800-100.

4.18.2 PL-2   SYSTEM SECURITY PLAN

Control: The organization:
   a.   Develops a security plan for the IS that:
      (1) Conforms to the SSP template as provided by the ISSM;
      (2) Is consistent with the enterprise architecture;
      (3) Explicitly defines the authorization boundary for the system;
      (4) Describes the operational context of the information system in terms of missions and business processes;
      (5) Describes the Concept of Operations (CONOPS) for the information system including, at a minimum, the purpose of the system and a description of the system architecture;
      (6) Provides the impact levels for Confidentiality, Integrity and Availability of the

information system including supporting rationale; and

    (7) Describes the functional architecture for the information system that identifies:

        (a) External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface.

        (b) User roles and the access privileges assigned to each role.

        (c) Unique security requirements.

        (d) Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders (EOs), directives, policies, regulations, standards, and guidance (to include any unique requirements of the Information Owner/Steward).

        (e) Restoration priority of information or information system services.

b. Describes the operational environment for the information system.

c. Describes relationships with or connections to other information systems, include ISAs and Authorizations to Connect (ATCs), as applicable;

d. Identifies the security requirements for the information system, as captured in the SSP;

e. Identifies controls tailored in or tailored out by the AO;

f. Identifies any exceptions, which denotes a control or part of a control that is not met and is an accepted risk by the AO. Exceptions should also be captured on the POA&M unless otherwise directed by the AO;

g. Identifies the type of control (common, system specific, or hybrid) and describes how the security controls are implemented or planned to be implemented including a rationale for any tailoring and supplementation decisions;

h. Identifies the controls tailored out/in/modified as approved by the AO;

i. Identifies any exceptions; i.e., a control or part of a control that is not or cannot be met and is an accepted risk by the AO. Exceptions shall also be included in the POA&M;

j. Approved by the AO ICW the SCA prior to the plan implementation;

k. Distributes copies of the plan and communicates subsequent changes to the plan to all required stakeholders, to include the AO;

l. Reviews the security plan at least annually or when required due to system changes or modifications;

m. Updates the plan to address changes to the IS/operations environment or problems identified during plan implementation or security control assessments; and

n. Protects the security plan from unauthorized disclosure and modification.

System Security Plans (SSPs) shall be classified in accordance with the Program SCG and in order to minimize OPSEC indicators.

Supplemental 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 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). Appendix I provide 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. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.

Organizations shall ensure an SSP is developed for each information system that:
  a. Identifies the tailored controls (tailored in/out/modified) approved by the AO.
  b. Identifies any exceptions, which denotes a control or part of a control that is not met and is an accepted risk by the AO. Exceptions should also be captured on the POA&M unless otherwise directed by the AO.
  c. Is approved by the AO through coordination with the SCA prior to plan implementation.

Information System Owner Responsibilities
The ISO is responsible for ensuring development and maintenance of the documentation for a security authorization package, to include the SSP.

The ISO shall ensure the SSP is reviewed at least annually and updated to address changes to the information system/environment of operation as well as problems identified during plan implementation or security control assessments.

Reference [CA-6] for examples of changes requiring SSP updates and Chapter 1 of this document for additional ISO responsibilities.

Control Enhancements:
4.18.2.1 PL-2(3) SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES
Control: The organization plans and coordinates security-related activities affecting the IS with all relevant organizations or groups before conducting such activities in order to reduce the impact on other organizational entities.

Supplemental 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. Related controls: CP-4, IR-4. References: NIST Special Publication 800-18.

4.18.3 PL-4 RULES OF BEHAVIOR
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 a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;

c. Reviews and updates the rules of behavior at least annually; and

d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

Rules of Behavior are addressed as part of user security awareness and training. See Security Training [AT-3]. Signed acknowledgement of the rules of behavior is covered via user access agreements. See User Agreements [PS-6]. The rules of behavior are also referred to as the Acceptable Use Policy (AUP). See the DAAPM for a list of the minimum responsibilities of a General User.

Supplemental 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 signed 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 for acknowledging rules of behavior. Related controls: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5.

Rules of Behavior are addressed as part of user security awareness and training [AT-3] as well as [PL-4]. Signed acknowledgement of the rules of behavior is covered via user access agreements. See User Agreements [PS-6].

The responsibilities of a General user shall include:

a. Reading and signing the Standard Mandatory Notice and Consent Provision for all DoD Information System User Agreements.

b. Use the system for official use only. Appropriate personal use of IS must be consistent with organizational policy.

c. Access only that data, system information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

d. Observe rules and regulations governing the secure operation and authorized use of IS.

e. Complete, at minimum, annual IA awareness training.

f. DO NOT introduce malicious code into any IS or physically damage the system.

g. DO NOT bypass, strain, or test security mechanisms. If security mechanisms must be bypassed for any reason, users shall coordinate with the ISSO and receive written permission from the ISSM to bypass security mechanisms.

h.   DO NOT introduce or use unauthorized software, firmware, or hardware on an IS.

i.   DO NOT relocate or change IS equipment or its network connectivity without proper security authorization.

j.   Secure unattended IS by invoking screen lock or logging off. Screen lock shall be employed for absences of a short duration. For any extended absence (more than six hours) and at the end of each workday, users are required to logout of all systems.

k.   Safeguard and report any unexpected or unrecognizable output products to the ISSO/SA as appropriate. This includes both displayed and printed products.

l.   Safeguard and report the receipt of any media received through any channel to the appropriate ISSO/SA for subsequent virus inspection and inclusion into the media control procedures. See also Media Access [MP-2].

m. Protect IS and IS peripherals located in the user's area from unauthorized access.

n.   Protect all authenticators (e.g., passwords, smart card personal identification numbers (PIN)/passwords, PKI private certificates) from disclosure to entities other than the user, system authentication components, and the authorized authenticator distribution entities. Single factor authenticators shall be protected commensurate with the information sensitivity accessible by the associated entity. Reference IA-5(6). Report any compromise or suspected compromise of an authenticator to the appropriate ISSO. Ensure all system media and output products are properly classified, marked, controlled, stored, transported, and destroyed. See also the Media Protection (MP) section.

o.   Immediately report all actual or suspected security incidents and potential threats and vulnerabilities involving an IS and/or network to the appropriate ISSO/SA or ISSM via secure means.

p.   DO NOT tamper with access doors, covers, plates and TEMPEST seals on IS.

q.   Inform the appropriate ISSO/SA when access to a particular IS is no longer required (e.g., completion of project, transfer, retirement, resignation).

r.   In addition to the requirements for a general user, privileged users shall:

(1) Access only the specific data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

(2) NOT use privileged user accounts to perform routine, non-administrative daily tasks (such as web browsing or reading electronic mail) as these activities may unintentionally damage or expose the system to attacks that are delivered via everyday applications.

(3) NOT use their privileged user accesses to alter, change or destroy information (e.g., audit logs, security-related objects and directories) without approval from the appropriate legal authority.

(4) Protect the "root" or "super user" authenticator at the highest level of data it secures.

(5) Use special accesses or permissions to perform only authorized tasks and functions.

(6) Take necessary precautions to protect the confidentiality of information encountered while performing privileged duties.

(7) Do not use special accesses or permissions to perform general user functions.

(8) Report and document all system security configuration changes and detected/suspected security-related IS problems that might adversely impact IS security to the ISSM.

Password Misuse or Compromise

Users shall take precautions to protect their passwords from misuse and compromise. A password shall be changed immediately if misuse or compromise of the password is known or suspected.

Suspected misuse or compromise of a password shall be reported to the ISSM/ISSO. Discovery of unauthorized use, possession, or downloading of a password-cracking tool shall be immediately reported to the ISSM/ISSO. Organizations shall establish procedures for all users to change their passwords, for example, in response to an incident affecting an information system resource, should such a response be required.

Control Enhancements:
4.18.3.1 PL-4(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING
RESTRICTIONS
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.

Supplemental 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 non-public organizational information (e.g., system account information, personally identifiable information) from social media/networking sites. References: NIST Special Publication 800-18.

4.18.4 PL-8   INFORMATION SECURITY ARCHITECTURE
Control: The organization:
  a. Develops an information security architecture for the IS that: describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity and availability of organizational information;
  b. Describes how the IS architecture is integrated into and supports the enterprise architecture; and describes any information security assumptions about, and dependencies on, external services;
  c. Reviews and updates the information security at least annually or when changes to the IS or its environment warrant to reflect updates in the enterprise architecture;
  d. Ensures that planned information security architecture changes are reflected in the security plan, the security CONOPS (if appropriate), and organizational procurements/acquisitions; and
  e. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

This control can be met through detailed descriptions in the SSP of the system overview, system environment, facility diagram, network architecture, system diagram, and system connectivity.

Supplemental Guidance: This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls),

security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs.

In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers.

Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e.; internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture. Related controls: CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, Appendix J.

Thorough detailed descriptions in the SSP of the system overview, system environment, facility diagram, network architecture, system diagram, and system connectivity can meet this control. See NIST Supplemental Guidance above for general contents of Information Security Architecture.

Control Enhancements:

4.18.4.1 PL-8(1) INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH

Control: The organization designs its security architecture using a defense in depth approach that allocates security safeguards based on security impact to Program IS; and ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.

Supplemental Guidance: Organizations strategically allocate security safeguards (procedural, technical, or both) in the security architecture so that adversaries have to overcome multiple safeguards to achieve their objective. Requiring adversaries to defeat multiple mechanisms makes it more difficult to successfully attack critical information resources (i.e., increases adversary work factor) and also increases the likelihood of detection. The coordination of allocated safeguards is essential to ensure that an attack that involves one safeguard does not create adverse unintended consequences (e.g., lockout, cascading alarms) by interfering with another safeguard. Placement of security safeguards is a key activity. Greater asset criticality or information value merits additional layering. Thus, an organization may choose to place anti-virus software at

organizational boundary layers, email/web servers, notebook computers, and workstations to maximize the number of related safeguards adversaries must penetrate before compromising the information and information systems. Related controls: SC-29, SC-36.

4.18.4.2 PL-8(2) INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY

Control: The organization requires that equipment and services to meet the security safeguards based on security impact to Program IS and its operational environment are obtained from different suppliers.

Supplemental Guidance: Different information technology products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors offering malicious code protection typically update their products at different times, often developing solutions for known viruses, Trojans, or worms according to their priorities and development schedules. By having different products at different locations (e.g., server, boundary, desktop) there is an increased likelihood that at least one will detect the malicious code. Related control: SA-12. References: None.

4.19   PERSONNEL SECURITY

4.19.1 PS-1   PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization:
  a. Develops, documents, and disseminates to **all personnel**:
     (1) A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
     (2) Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
  b. Reviews and updates the current:
     (1) Personnel security policy **at least annually**; and
     (2) Personnel security procedures **at least annually**.

Supplemental 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. Related control: PM-9.

Specific policy and procedures related to personnel security are defined in the remainder of this section.

Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.

4.19.2 PS-2   POSITION RISK DESIGNATION

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 updates position risk designations [Annually].

Access to individual Programs will be managed in accordance with NISPOM). Positions will be reviewed annually or as policy and procedures dictate changes are required.

Supplemental 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). Related controls: AT-3, PL-2, PS-3.
Key Management Personnel designation shall be reviewed annually.

Control Enhancements: None. References: 5 C.F.R. 731.106.
4.19.3 PS-3   PERSONNEL SCREENING
Control: The organization:
    a. Screens individuals prior to authorizing access to the information system.
    b. Rescreens individuals according to personnel security guidelines defined.

Organizations shall ensure that every user accessing an IS processing, storing, or transmitting types of classified information which require formal indoctrination, is formally indoctrinated for all information for which the user is authorized access.

Supplemental 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. Related controls: AC-2, IA-4, PE-2, PS-2.

Control Enhancements:
4.19.3.1 PS-3(1) PERSONNEL SCREENING | CLASSIFIED INFORMATION
Control: The organization ensures that individuals accessing an information system processing, storing, or transmitting types of classified information which require formal indoctrination, are formally indoctrinated for all of the relevant types of information to which they have access on the system. Supplemental Guidance: none. Related controls: AC-3, AC-4.

4.19.4 PS-4   PERSONNEL TERMINATION
Control: The organization, upon termination of an individual:
    a. Disables information system access within 24 hours;
    b. Terminates/revokes any authenticators/credentials associated with the individual;
    c. Conducts exit interviews that include a discussion of any prohibitions regarding the information obtained during the employment;
    d. Retrieves all security-related organizational information system-related property;
    e. Retains access to organizational information and information systems formerly controlled by terminated individual; and
    f. Notifies the ISSM immediately upon termination.

When any system user (to include privileged and non-privileged users) leaves the organization due to employment termination (whether voluntary of involuntary) or retirement, the responsible

for user account management must ensure all system accesses are removed. This includes notifying other organizations that may have granted system accesses (for example, collateral systems access, database access managed by another agency or organization, etc.).

Notification of an employee's termination is the responsibility of the organization. The organization must also ensure that information deemed to be of value is retained before the departing user's accounts are archived and removed. The property custodian must retrieve any equipment issued to the departing individual, such as laptops or PEDs. The loss of security clearance or formal access approval (through de-briefing, suspension or revocation) requires immediate deactivation of all accounts associated with the individual.

Supplemental 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 non-availability 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. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.

Control Enhancements:
4.19.4.1 PS-4(1) PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS
Control: The organization:
- a. Notified termination individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and
- b. Requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.

Supplemental Guidance: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

4.19.5 PS-5   PERSONNEL TRANSFER
Control: The organization, upon transfer of an individual:
- a. Reviews and confirms any 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 reassignment actions to ensure all system access no longer required (need to know) are removed or disabled within 10 working days;
- c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
- d. Notifies the ISSM as soon as possible.

Notify other organizations that may have granted system accesses (for example, collateral systems access, database access managed by another agency or organization) of the individual's transfer or reassignment. Notification of an employee's transfer or reassignment shall be documented as the responsibility of the employee's supervisor or Human Resources. The property custodian must determine whether any equipment issued to the individual, such as laptops or PEDs, should be retrieved or transferred to another property account. Reference AC-2 for additional requirements.

Supplemental 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. Related controls: AC-2, IA-4, PE-2, PS-4.

Control Enhancements: None. References: None.
4.19.6 PS-6   ACCESS AGREEMENTS
Control: The organization:
- a. Develops and documents access agreements for organizational information systems;
- b. Reviews and updates the access agreements **at least annually**; and
- c. Ensures that individuals requiring access to organizational information and information systems:
    - (1) Sign appropriate access agreements prior to being granted access; and
    - (2) Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or **at least annually.**

Supplemental 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.
Related control: PL-4, PS-2, PS-3, PS-4, PS-8.

Agreement and Acknowledgement of Responsibilities prior to being granted elevated privileges to IS and applications. These agreements must be reviewed and updated upon account creation, user transfer or user termination. Organizations may add additional requirements to the agreement provided they do not conflict with the official verbiage. See Account Management [AC-2] for additional information on user roles and responsibilities.

All users are required to read and sign a Standard Mandatory Notice and Consent provision for all IS, (i.e., General User Access Agreement and Acknowledgement of Responsibilities) prior to being granted access to information systems. In addition, privileged users are required to read and sign a Privileged User Access.

The User Access Agreement shall be retained by the ISSM/SA for a minimum of two years after access is removed.

Organizations shall ensure that access to any information with special protection measures is granted only to individuals who:
   a. Have a valid access authorization that is demonstrated by assigned official government duties.
   b. Satisfy associated personnel security criteria consistent with applicable federal laws, EOs, directives, policies, regulations, standards, and guidance.
   c. Have read, understand, and signed a nondisclosure agreement (if applicable).

Control Enhancements:
4.19.6.1 PS-6(2) ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION
Control: The organization ensures that access to classified information requiring special protection is granted only to individuals who (a) have a valid access authorization that is demonstrated by assigned official government duties; (b) satisfy associated personnel security criteria; and (c) have read, understood, and signed a nondisclosure agreement.

Supplemental Guidance: Classified information requiring special protection includes, for example, collateral information,). Personnel security criteria reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

4.19.6.2 PS-6(3) ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS
Control: The organization:
   a. Notifies individuals of applicable, legally-binding post-employment requirements for protection of organizational information; and
   b. Requires individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

Supplemental Guidance: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals. References: None.

4.19.7 PS-7   THIRD-PARTY PERSONNEL SECURITY
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 the organization of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges as soon as possible, but not to exceed one working day; and
   e. Monitors provider compliance.

The term "third party" as it relates to personnel security and contracts is not frequently used in DoD. If a third-party situation seems to apply, contact the AO and/or contracting representative for clarification and guidance. For Army: ensure DSS contacted if appropriate.

Supplemental 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. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.

The term 'third party' as it relates to Personnel Security and contracts is not frequently used in DoD. If a third-party situation seems to apply, contact your AO-designated representative

Control Enhancements: None. References: NIST Special Publication 800-35.

4.19.8 PS-8   PERSONNEL SANCTIONS

Control: The organization:
   a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
   b. Notifies the appropriate organizations as soon as possible when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

All instances where an individual fails to comply with established information security policies and procedures will be treated as security incidents.

Supplemental 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. Related controls: PL-4, PS-6.

All instances where an individual fails to comply with established information security policies and procedures will be treated as security incidents and handled in accordance with User Agreement.

Control Enhancements: None. References: None.

4.20   RISK ASSESSMENT

4.20.1 RA-1   RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:
   a. Develops, documents, and disseminates to [at minimum, the ISSM and ISSO]:
      (1) A Risk assessment policy that addresses purpose, scope responsibilities, management commitment, coordination among organizational entities, and compliance;
      (2) Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
   b. Reviews and updates the current
      (1) Risk assessment policy annually; and
      (2) Risk assessment procedures annually.

Supplemental 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. Related control: PM-9.

Specific policy and procedures related to risk assessment are defined in the remainder of this section.

Control Enhancements: None. References: NIST Special Publications 800-12, 800-30, 800-100.

4.20.2 RA-2 SECURITY CATEGORIZATION
Control: The organization:
  a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, and directives, policies, regulations, standards, and guidance;
  b. Documents the security categorization results (including supporting rationale) in the SSP for the information system; and
  c. Ensures that the security categorization decision is reviewed by the SCA/ISSP and approved by the AO/AO Representative.

The ISSM shall work with Program in determining the appropriate security categorization as part of the initial preparatory actions prior to selecting and tailoring the security controls.

Supplemental 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 senior information security officers, information system owners, mission/business owners, and information owners/stewards and IO approval. 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. Related controls: CM-8, MP-4, RA-3, SC-7.

Control Enhancements: None. References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.

4.20.3 RA-3 RISK ASSESSMENT
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 Risk Assessment Report;

c.   Reviews risk assessment results at least annually;

d.   Disseminates risk assessment results to the SCA/ISSP for initial review and to the AO/AO Representative for final approval; and

e.   Updates the risk assessment at least annually 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 state of the system.

The RAR is part of the required Body of Evidence (BoE) provided to the AO as the basis of the authorization to operate decision. The RAR should be initiated prior to or during Step 1, Security Categorization.

Supplemental 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. Related controls: RA-2, PM-9.

Organizations shall conduct a risk assessment for each system under their purview. The risk assessment shall address the likelihood and magnitude of harm resulting from the unauthorized disclosure, modification or denial of availability of the system and the information it processes, stores, or transmits. The risk assessment shall take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, other organizations, and national security based on the operation of the system. The risk assessment shall also take into account risk to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors' operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities). A clearly defined authorization boundary is a prerequisite for an effective risk assessment.

Risk assessments (either formal or informal) can be conducted by organizations at various steps in the RMF including:

a.   IS categorization;

b.   Security control selection;
c.   Security control implementation;
d.   Security control assessment;
e.   IS authorization; and
f.   Security control monitoring.

Risk assessments help senior management make decisions on policy, procedural, budget, and system operational and management changes. Risk assessments shall be initiated by ISOs during Step 1 of the RMF, Security Categorization. The initial risk assessment will evaluate anticipated security vulnerabilities affecting confidentiality, integrity, and availability of the system in the context of the planned operational environment. The initial risk assessment will conclude with recommendations for appropriate security safeguards, permitting management to make knowledge-based decisions about the security controls necessary to properly secure the system based on its categorization and threat environment.

Results from the initial risk assessment shall be documented in a separate RAR or in the SSP. The RAR shall include the vulnerabilities, threats, threat sources, other conditions that may affect the security of the system, and any residual risk incurred by operating the system as identified in the SSP.

The RAR shall be updated during later stages in the RMF and is an important part of the security authorization package. The risk assessment process is revisited, as necessary, throughout the RMF to provide the AO with an updated risk picture reflecting the actual (versus planned) state of affairs with regard to system implementation, security control effectiveness, and the operational environment. The RAR for the as-built or as-deployed system shall include a description of the known vulnerabilities in the system, an assessment of the risk posed by each identified vulnerability, and corrective actions that can be taken to mitigate the risks. It shall also include an assessment of the overall risk to the organization and the information contained in the system by operating the system as evaluated.

The SCA is responsible for reviewing the RAR and providing feedback to the ISO regarding the completeness of the risk assessment and appropriateness of planned safeguards.

The risk assessment and associated RAR must be reviewed and updated at least annually or whenever there are significant changes to the IS or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Control Enhancements: None.
References: OMB Memorandum 04-04; NIST Special Publications 800-30, 800-39; Web:
http://idmanagement.gov.
4.20.4 RA-5 VULNERABILITY SCANNING
Control: The organization:
a.   Scans for vulnerabilities in the information system and hosted applications at least monthly 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 guidance provided by MOU/ISA or AO in accordance with an organizational assessment of risk;

e. Shares information obtained from the vulnerability scanning process and security control assessments with the AO/AO Representative and the SCA/ISSP to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies);

f. Updates the POA&M with true vulnerabilities identified during scanning; and

g. Information revealing specific vulnerabilities (other than the known vulnerabilities of widely available commercial products) and the compiled results of vulnerability analyses for systems shall be classified in accordance with the applicable SCG.

This control may be tailored out.

When feasible or required by contract and/or ISA/MOU, organizations shall use vulnerability assessment tools (e.g., Assured Compliance Assessment Solution (ACAS). The ISSM/ISSO shall analyze vulnerability scans to determine true vs. false positives. True vulnerabilities identified as part of a scan shall be added to the POA&M.

Supplemental 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). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.

Organizations shall use AO-approved vulnerability assessment tools and procedures on all systems to include weapon systems, satellite systems, networks, information systems and system applications, as appropriate. Vulnerability assessment tools shall have the capability to readily update the list of system vulnerabilities scanned.

Security Classification Guides should address the protection of information revealing specific vulnerabilities (other than the known vulnerabilities of widely available commercial products) and the compiled results of vulnerability analyses for systems. This information's confidentiality requires protection and access to this information must be controlled in accordance with SCG.

The ISSM/ISSO will ensure analysis of all vulnerability scan reports to determine whether reported vulnerabilities apply to the system. Some of the potential vulnerabilities reported by automated scanning tools may not represent real vulnerabilities in the context of the system environment. For example, some of the "vulnerabilities" flagged by the automated scanning software may not be applicable for a particular site (i.e., they may be false positives).

Organizations shall attempt to discern what information about the system is discoverable by adversaries, document the information and determine potential risk.

The ISSM/ISO is responsible for ensuring all vulnerabilities are remediated based on guidance provided by the AO. The ISO shall develop and maintain POA&Ms to address all vulnerabilities identified by scanning.

Reference Incident Monitoring [IR-5] for more information on IAVM.

Control Enhancements:
4.20.4.1 RA-5(1) VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY
Control: The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

This control may be tailored out.

When feasible or required by contract and/or ISA/MOU, organizations shall use vulnerability assessment tools (E.g. Assured Compliance Assessment Solution (ACAS) The ISSM/ISSO shall analyze vulnerability scans to determine true vs. false positives. True vulnerabilities identified as part of a scan shall be added to the POA&M.

Supplemental 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. Related controls: SI-3, SI-7.

4.20.4.2 RA-5(2) VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED
Control: The organization updates the information system vulnerabilities scanned as new automated tool scripts are issued; within 30 days prior to running scans; prior to a new scan; when new vulnerabilities are identified and reported. This control supports insider threat mitigation. Supplemental Guidance: Related controls: SI-3, SI-5.

4.20.4.3 RA-5(4) VULNERABILITY SCANNING | DISCOVERABLE INFORMATION
Control: The organization determines what information about the information system is discoverable by adversaries and subsequently documents the information, determines potential risk, and takes corrective action to mitigate the vulnerabilities.

Supplemental Guidance: Discoverable information includes information that adversaries could obtain without directly compromising or breaching the information system, for example, by collecting information the system is exposing or by conducting extensive searches of the web. Corrective actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the information system to make designated information less relevant or attractive to adversaries. Related control: AU-13.

4.20.4.4 RA-5(5) VULNERABILITY SCANNING | PRIVILEGED ACCESS

Control: Organizations shall provide privileged access authorization to all systems and infrastructure components for vulnerability scanning activities to facilitate more thorough scanning.

Supplemental 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.

4.20.5 RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

Control: The organization employs a technical surveillance countermeasures survey at their facilities as required.

Supplemental Guidance: Technical surveillance countermeasures surveys are performed by qualified personnel to detect the presence of technical surveillance devices/hazards and to identify technical security weaknesses that could aid in the conduct of technical penetrations of surveyed facilities. Such surveys provide evaluations of the technical security postures of organizations and facilities and typically include thorough visual, electronic, and physical examinations in and about surveyed facilities. The surveys also provide useful input into risk assessments and organizational exposure to potential adversaries. Control Enhancements: None. References: None.

4.21   SYSTEM AND SERVICES ACQUISITION

4.21.1 SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization:
   a. Develops, documents, and disseminates to [all personnel]:
      (1) A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
      (2) Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls;
      (3) Reviews and update and services acquisition policy [annually]; and
      (4) System and services acquisition procedures annually.

Supplemental 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. Related control: PM-9.

Specific policy and procedures related to system and services acquisition are defined in the remainder of this section.

Control Enhancements: None.
References: NIST Special Publications 800-12, 800-100.
4.21.2 SA-2   ALLOCATION OF RESOURCES
Control: The organization:
- a. Determines information security requirements for the IS or IS service in mission/business process planning;
- b. Determines, documents, and allocates the resources required to protect the IS or IS service as part of its capital planning and investment control process; and
- c. Establish a discrete line item for information security in organizational programming and budgeting documentation.

When applicable, Statements of Work (SOWs) will include a DD Form 254 and address contractor-related security issues including, but not limited to:
- a. Personnel security.
- b. Physical security.
- c. Information systems in support of the contract.
- d. TEMPEST requirements.
- e. Applicable security regulations.

Supplemental 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. Related controls: PM-3, PM-11.

As applicable, SOWs will include a DD Form 254 and address contractor-related security issues including, but not limited to:
- a. Personnel security.
- b. Physical security.
- c. Information systems in support of the contract.
- d. TEMPEST requirements.
- e. Applicable security regulations.
- f. A Government official will coordinate these specific requirements depending upon the particular acquisition.

Control Enhancements: None.
References: NIST Special Publication 800-65.
4.21.3 SA-3 SYSTEM DEVELOPMENT LIFE CYCLE
Control: The organization:
- a. Manages information systems using a System Development Life Cycle (SDLC) methodology that incorporates information security considerations;
- b. Defines and documents information security roles and responsibilities throughout the SDLC;
- c. Identify individuals having information security roles and responsibilities; and
- d. Integrate the organizational information security risk management process into system development life cycle activities.

Supplemental 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. Related controls: AT-3, PM-7, SA-8.

Control Enhancements: None. References: NIST Special Publications 800-37, 800-64.
4.21.4 SA-4 ACQUISITION PROCESS
Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contracts for the IS, system component, or IS service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational business/mission 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.

Supplemental 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 Federal Information Security Management Act of 2002 (FISMA). Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.

Control Enhancements:
4.21.4.1 SA-4(1) ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS
Control: The organization requires the developer of the IS, system component, or the IS service to provide a description of the functional properties of the security controls to be employed. The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within information systems with sufficient detail to permit analysis and testing.

Supplemental 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. Related control: SA-5.

Obtain, protect as required, and make available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within information systems with sufficient detail to permit analysis and testing.

4.21.4.2 SA-4(2) ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS
Control: The organization requires the developer of the IS, system component, or IS service to provide design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces; high level design; source code or hardware schematics and other system or service specific implementation information at a sufficient level of detail.

Supplemental 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. Related control: SA-5.

Require in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within information systems, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.

4.21.4.3 SA-4(6) ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS

Control: The organization:
   a. Shall employ only Government-of-the-Shelf (GOTS) or COTS IA and IA-enabled IT products that compose an NSA-approved solution to protect classified information when the system(s)/networks used to process, store, and/or transmit the information are at a lower classification level than the information being transmitted (i.e., tunneling) [SA-4(6)(a)]; and
   b. Ensure that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.

Supplemental Guidance: COTS IA or IA-enabled information technology products used to protect classified information by cryptographic means may be required to use NSA-approved key management. Related controls: SC-8, SC-12, SC-13.

4.21.4.4 SA-4(7) ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES

Control: The organization:
   a. Limits the use of commercially provided IA and IA-enabled IT products to those products that have been successfully evaluated against a 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 IT products relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.

Supplemental Guidance: Related controls: SC-12, SC-13.

4.21.4.5 SA-4(9) ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE

Control: The organization requires the developer of the IS, system component, or IS service to identify early in the SDLC, the functions, ports, protocols, and services intended for organizational use. This allows the organization the opportunity to influence the design of the IS, IS component or IS service to prevent unnecessary risks.

Supplemental 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. Related controls: CM-7, SA-9.

4.21.4.6 SA-4(10) ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS

Control: The organization employs only IT products on the FIPS 201-approved products list for PIV (also known as CAC) capability implemented within organization information systems.

Supplemental Guidance: Related controls: IA-2; IA-8. References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: http://www.niap-ccevs.org, http://fips201ep.cio.gov, http://www.acquisition.gov/far.

4.21.5 SA-5   INFORMATION SYSTEM DOCUMENTATION

Control: The organization:
   a. Obtain administrator documentation for the IS, IS component, or IS service that describes:
      (1) Secure configuration, installation, and operation of the information system;
      (2) Effective use and maintenance of security features/functions; and
      (3) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
   b. Obtain user documentation for the IS, IS component, or IS service that describes:
      (1) User-accessible security features/functions and how to effectively use those security features/functions;
      (2) Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner (e.g. training materials, user guides, Standard Operating Procedures); and
      (3) User responsibilities in maintaining the security of the information and information system.
   c. Document attempts to obtain IS, IS component, or IS service documentation when such documentation is either unavailable or nonexistent;
   d. Protects documentation as required, in accordance with the risk management strategy; and
   e. Distributes documentation to stakeholders.

Supplemental 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. 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. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.

Control Enhancements:
4.21.6 SA-8   SECURITY ENGINEERING PRINCIPLES
Control: Organizations shall apply information system security engineering principles in the specification, design, development, implementation, and modification of information systems.

Examples of security engineering principles include, but are not limited to:
   a. Developing layered protections;
   b. Establishing sound security policy, architecture, and controls as the foundation for design; Incorporating security into the SDLC;
   c. Delineating physical and logical security boundaries;
   d. Ensuring system developers and integrators are trained on how to develop secure software;
   e. Tailoring security controls to meet organizational and operational needs; and
   f. Reducing risk to acceptable levels, thus enabling informed risk management decisions.

Supplemental 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; 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. Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.

The ISSM and the respective ISO shall ensure the IS security design meets the applicable security requirements.

For legacy information systems (e.g., legacy OS), organizations shall apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system.

Control Enhancements: None. References: NIST Special Publication 800-27.
4.21.7 SA-9   EXTERNAL INFORMATION SYSTEM SERVICES
Control: The organization:
   a. Require that providers of External Information System services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, EOs, 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 appropriate processes and/or technologies to monitor security control compliance by external service providers on an ongoing basis.

External Information System services are service that are implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of External Information System services remains with the AO. When a sufficient level of trust cannot be established in the external services and/or service providers, the organization shall employ compensating security controls or accept the greater degree of risk.

Supplemental 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. Related controls: CA-3, IR-7, PS-7.

Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization shall employ compensating security controls or accept the greater degree of risk.

Control Enhancements:
4.21.7.1 SA-9(1) EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS
Control: The organization:
    a. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and
    b. Ensures the acquisition or outsourcing of dedicated information security services is approved as defined at the system or program level. Organizations should ensure that individuals with the regulatory and organizational authority to outsource services conduct full scope risk assessments and ensure that appropriate individuals are involved in this decision. This approval line can be reserved for CIO, AO, or contracting officer as appropriate based on an organization's structure. 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.

Supplemental Guidance: 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. Related controls: CA-6, RA-3.

4.21.7.2 SA-9(2) EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES

Control: The organization requires providers of all external information systems and services to identify the functions, ports, protocols, and other services required for the use of such services.

Supplemental 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. Related control: CM-7.

4.21.8 SA-10   DEVELOPER CONFIGURATION MANAGEMENT

Control: The organization shall require that IS developers/integrators of the IS, system component of IS service to:
    a. Perform configuration management during IS, system component of IS service design development, implementation and operation;
    b. Document, manage, and control the integrity of changes to IS, system component of IS services;
    c. Implement only organization-approved changes to the IS, system component of IS service;
    d. Document approved changes to the IS, system component of IS service and the potential security impacts of such changes; and
    e. Track security flaws and flaw resolution within the IS, system component of IS service and report vulnerabilities to the ISSM/ISSO.

This control also applies to organizations conducting internal information systems development and integration. 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.

Supplemental 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. Related controls: CM-3 , CM-4, CM-9, SA-12, SI-2.

Control Enhancements:
4.21.8.1 SA-10(1) DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION
Control: The organization requires the developer of the IS, system component, or IS service to enable integrity verification of software and firmware components.

Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to software and firmware components through the use of tools, techniques, and/or mechanisms provided by developers. Integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components. Related control: SI-7.

4.21.9 SA-11 DEVELOPER SECURITY TESTING AND EVALUATION
Control: The organization requires the developer of the IS, system component, or information system service to:
  a. Create and implement a security assessment plan;
  b. Perform the appropriate type of testing/evaluation (e.g., unit, integration, system, regression);
  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. Document the results of the security testing/evaluation and flaw remediation processes.

Security testing and evaluation will be conducted in consultation with security personnel (e.g., ISSM/ISSO). An objective of the flaw remediation process is to correct weaknesses and deficiencies identified during the security testing and evaluation process.

Supplemental Guidance: Developmental security testing/evaluation occur 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. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

Security testing and evaluation will be conducted, in consultation with associated security personnel (including security engineers):
   a. An objective of the flaw remediation process is to correct weaknesses and deficiencies identified during the security testing and evaluation process.
   b. The results of the security testing/evaluation and flaw remediation process should be documented.

4.21.10 SA-12 SUPPLY CHAIN PROTECTION
Control: Organizations shall conduct a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services, including a review of supplier claims with regard to the use of appropriate security processes in the development and manufacture of IS components or products.

Organizations protects against supply chain threats to the IS, system component, or IS service by employing security safeguards in accordance with CNSSD No. 505, Supply Chain Risk Management as part of a comprehensive, defense-in-depth information security strategy.

Supplemental Guidance: 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. Related controls: AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7.

4.21.11 SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control: The organization:
   a. Requires the developer if the IS, system component, or IS service to follow a documented process that:
      (1) Explicitly addresses security requirements;
      (2) Identifies the standards and tools used in the development process;
      (3) Documents the specific tool options and tool configuration used in the development process; and
      (4) Documents, manages, and ensures the integrity of changes to the process and/or tools used in the development.
   b. Reviews the development process, standards, tools, and tool options/configurations regularly but no less than annually to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy organizational security requirements.

Supplemental Guidance: Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes. Related controls: SA-3, SA-8.

Control Enhancements:
4.21.11.1   SA-15(9) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | USE OF LIVE DATA

Control: The organization approves, documents, and controls the use of live data in development and test environments for the IS, system component, or IS service.

Supplemental Guidance: The use of live data in preproduction environments can result in significant risk to organizations. Organizations can minimize such risk by using test or dummy data during the development and testing of information systems, information system components, and information system services.

4.21.12 SA-19 COMPONENT AUTHENTICITY

Control: The organization:
   a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the IS; and
   b. Reports counterfeit IS components to DSS.

Supplemental Guidance: Sources of counterfeit components include, for example, manufacturers, developers, vendors, and contractors. Anti-counterfeiting policy and procedures support tamper

resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include, for example, US-CERT. Related controls: PE-3, SA-12, and SI-7.

4.21.13 SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization:
   a. Develops, documents, and disseminates to **[at a minimum, the ISSM/ISSO]**:
      (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.
   b. Reviews and updates the current:
      (1) System and communications protection policy **[annually]**; and
      (2) System and communications protection procedures **[annually]**.

Supplemental 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. Related control: PM-9.

Specific policy and procedures related to system and communications protection are defined in the remainder of this section.

Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.

4.21.14 SC-2 APPLICATION PARTITIONING

Control: The IS separates user functionality (including user interface services) from information system management functionality.

Application partitioning is separating an application physically or logically into components that run on multiple servers. This provides additional security by separating specific IS management from general user functionality, as well as load balancing across the enterprise.

Supplemental 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. Related controls: SA-4, SA-8, SC-3.

4.21.15 SC-3 SECURITY FUNCTION ISOLATION

Control: The IS isolates security function from non-security functions. The information system isolates security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains). Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

Supplemental Guidance: The information system isolates security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains). Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions.

Information systems implement code separation (i.e., separation of security functions from non-security functions) in a number of ways, including, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk, and address space protections that protect executing code. Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities. While the ideal is for all of the code within the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include non-security functions within the isolation boundary as an exception. Related controls: AC-3, AC-6, SA-4, SA-5, SA-8, SA-13, SC-2, SC-7, SC-39.

Security function isolation includes, but is not limited to, audit daemons, host-based firewalls, anti-virus or filtering functions, and account management.

4.21.16 SC-4 INFORMATION IN SHARED RESOURCES

Control: The IS prevents unauthorized and unintended information transfer via shared system resources.

Supplemental 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. Related controls: AC-3, AC-4, MP-6. See PE-5 for KVM guidance.

4.21.17 SC-5 DENIAL OF SERVICE PROTECTION

Control: The IS protects against or limits the effects of denial of service attacks.

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. Supplemental 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. Related controls: SC-6, SC-7.

Control Enhancements:
4.21.17.1   SC-5(1) DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS
Control: The IS restricts the ability of individuals to launch denial of service attacks against other IS.

Protection against individuals having the ability to launch denial of service attacks may be implemented on specific information systems or on boundary devices prohibiting egress to potential target systems.

Supplemental Guidance: Restricting the ability of individuals to launch denial of service attacks requires that the mechanisms used for such attacks are unavailable. Individuals of concern can include, for example, hostile insiders or external adversaries that have successfully breached the information system and are using the system as a platform to launch cyber-attacks on third parties. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., network, wireless spectrum). Organizations can also limit the ability of individuals to use excessive information system resources. Protection against individuals having the ability to launch denial of service attacks may be implemented on specific information systems or on boundary devices prohibiting egress to potential target systems.

4.21.18 SC-7 BOUNDARY PROTECTION
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 physically and 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 organizational security architecture.

This requirement also applies to ports, protocols, and services. Information systems, in conjunction with the environment in which they are installed, shall:
   a. Provide for remote access only for an authorized, specific purpose (for example, to provide email access for a guest agency's employee via a VPN). The remote connection must be restricted to approved purposes. Authorized remote access shall not enable the user to communicate as an extension of the IS or to communicate with local resources such as a printer or file server unless explicitly authorized by the AO;

      b.   Route specific internal communications traffic through authenticated proxy servers within the managed interfaces of boundary protection devices, to external networks (i.e., networks outside the control of the organization). The list of traffic to be routed through managed interfaces may be augmented with service/agency or site-specific requirements and approved by the AO or designee;

    c. Use private/non-publicly routable IP addresses for isolated LANs; and

    d. Host-based boundary protection mechanisms shall be employed on mobile devices, (e.g., notebook/laptop computers and other types of mobile devices) where boundary protection mechanisms are available. This typically applies when your internal network has classification or access levels that differ.

Supplemental 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 Demilitarized Zones (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. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.

This requirement also applies to ports, protocols, and services.

Information systems, in conjunction with the environment in which they are installed, shall:

    a. Provide for remote access only for an authorized, specific purpose (for example, to provide email access for a guest agency's employee via a VPN). The remote connection must be restricted to approved purposes. Authorized remote access shall not enable the user to communicate as an extension of the IS or to communicate with local resources such as a printer or file server unless explicitly authorized by the AO;

    b. Route specific internal communications traffic through authenticated proxy servers within the managed interfaces of boundary protection devices, to external networks (i.e., networks outside the control of the organization). The list of traffic to be routed through managed interfaces may be augmented with service/agency or site-specific requirements and approved by the AO or designee;

    c. Use private/non-publicly routable IP addresses for isolated LANs; and

    d. Host-based boundary protection mechanisms shall be employed on mobile devices, (e.g., notebook/laptop computers and other types of mobile devices) where boundary protection mechanisms are available. This typically applies when your internal network has classification or access levels that differ.

Control Enhancements:
4.21.18.1   SC-7(3) BOUNDARY PROTECTION | ACCESS POINTS
Control: The organization:

a.   Limits the number of external network connections to the information system and prevents public access into the organization's internal networks except as allowed by managed interfaces employing boundary protection devices. This control generally applies when the system is connected to unclassified system.

Physically allocate publicly accessible information system components to separate sub-networks with separate physical network interfaces. Publicly accessible information system components include, for example, public web servers.

Limits the number of access points to information systems under their purview to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

Supplemental 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.

4.21.18.2   SC-7(4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES

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 information being transmitted across each interface;
   d. Documents exceptions to the traffic flow policy with a supporting mission/business need and the duration of that need in the SSP; and
   e. Reviews exceptions to the traffic flow policy at least annually; Eliminates traffic flow policy exceptions that are no longer required by an explicit mission/business need; and update the SSP accordingly.

Supplemental Guidance: Related control: SC-8.

4.21.18.3   SC-7(5) BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION

Control: The organization at managed interfaces denies network traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception). This requirement applies to ports, protocols, and services.

Supplemental 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.

4.21.18.4   SC-7(7) BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES

Control: The IS, 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.

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.

Supplemental 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.

4.21.18.5   SC-7(8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

Control: The IS routes specific internal communications traffic through authenticated proxy servers within the managed interfaces of boundary protection devices, to external networks (i.e., networks outside the control of the organization). The list of traffic to be routed through managed interfaces may be augmented with Service or site-specific requirements and approved by the AO or designee.

Supplemental Guidance: 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 addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Related controls: AC-3, AU-2.

4.21.18.6   SC-7(9) BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC

Control: The information system:
   a. Detects and denies outgoing communications traffic posing a threat to external information systems; an detects and denies outgoing communications traffic posing a threat to external IS; and
   b. Audits the identity of internal users associated with denied communications.

This is sometimes termed extrusion detection and includes traffic indicative of denial of service attacks and traffic containing malicious code.

Supplemental Guidance: Detecting outgoing communications traffic from internal actions that may pose threats to external information systems is sometimes termed extrusion detection. Extrusion detection at information system boundaries as part of managed interfaces includes the analysis of incoming and outgoing communications traffic searching for indications of internal threats to the security of external systems. Such threats include, for example, traffic indicative of denial of service attacks and traffic containing malicious code. Related controls: AU-2, AU-6, SC-38, SC-44, SI-3, SI-4.

4.21.18.7   SC-7(10) BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION

Control: The organization prevents the unauthorized exfiltration of information across managed interfaces.

Supplemental Guidance: Safeguards implemented by organizations to prevent unauthorized exfiltration of information from information systems include, for example: (i) strict adherence to protocol formats; (ii) monitoring for beaconing from information systems; (iii) monitoring for steganography; (iv) disconnecting external network interfaces except when explicitly needed; (v) disassembling and reassembling packet headers; and (vi) employing traffic profile analysis to detect deviations from the volume/types of traffic expected within organizations or call backs to command and control centers. Devices enforcing strict adherence to protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to protocol formats and specification at the application layer and serve to identify vulnerabilities that cannot be detected by devices operating at the network or transport layers. This control enhancement is closely associated with cross-domain solutions and system guards enforcing information flow requirements. Related control: SI-3.

4.21.18.8   SC-7(11) BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC

Control: The IS only allows incoming traffic from authorized sources routed to an authorized destination.

Supplemental Guidance: This control enhancement provides determinations that source and destination address pairs represent authorized/allowed communications. Such determinations can be based on several factors including, for example, the presence of source/destination address pairs in lists of authorized/allowed communications, the absence of address pairs in lists of unauthorized/disallowed pairs, or meeting more general rules for authorized/allowed source/destination pairs. Related control: AC-3.

4.21.18.9   SC-7(12) BOUNDARY PROTECTION | HOST-BASED PROTECTION

Control: The organization implements host-based boundary protection mechanisms (e.g., a host-based firewall) for servers, workstations, and mobile devices. Host-based boundary protection mechanisms shall be employed on mobile devices, (e.g., notebook/laptop computers and other types of mobile devices) where boundary protection mechanisms are available. This typically applies when the internal network has classification or access levels that differ.

Supplemental Guidance: 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.

4.21.18.10   SC-7(13) BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS

Control: The organization isolates, at a minimum, vulnerability scanning tools, audit log servers, patch servers, and Computer Network Defense (CND) tools from other internal information system components via physically separate subnets with managed interfaces to other system or network components.

Supplemental Guidance: 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. Related controls: SA-8, SC-2, SC-3.

4.21.18.11   SC-7(14) BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS

Control: The organization protects against unauthorized physical connections at any managed interface that crosses security domains or connects to an external network; such as, but not limited to cross domain solutions, a network boundary with a WAN, a partner network, or the Internet.

Supplemental Guidance: Information systems operating at different security categories or classification levels may share common physical and environmental controls, since the systems may share space within organizational facilities. In practice, it is possible that these separate information systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved, for example, by employing clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls enforcing limited authorized access to these items. Related controls: PE-4, PE-19. Reference also SC-8.

4.21.19 SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control: The IS protects the confidentiality and integrity of transmitted information. 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). When more than one computer network exists, a color coding scheme shall be developed to assist in the proper handling of classified information. Color coding of cables may be met by any of the following:
   a.   Purchasing/making cables with the proper color;
   b.   Placing colored tape every five feet along the cable length;
   c.   Wrapping tape around the length of the cable run; and
   d.   Cable labeling.

When networks are present other than those listed above, a different color must be selected for the network cables to assist in minimizing the risk to classified IS.

Supplemental 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 protected 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. Related controls: AC-17, PE-4.

This control prevents information from being modified at data aggregation or protocol transformation points, compromising the integrity of the information.

A PDS must be used to transmit unencrypted classified information though an area of lesser classification or control. For additional information, and where NIST referenced National Security Telecommunications and Information Systems, see CNSSI 7003,

Protective Distribution Systems
When more than one computer network exists within a Closed Area, a color coding scheme shall be developed to assist in the proper handling of classified information.
For additional information see Appendix P.

Control Enhancements:
4.21.19.1   SC-8(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION
Control: The information system implements cryptographic mechanisms to prevent unauthorized disclosure of, and detect changes to, information during transmission unless otherwise protected by alternative physical safeguards such as keeping transmission within physical areas rated in accordance with the sensitivity of the information or within a PDS when traversing areas not approved for the sensitivity of the information. This applies to sensitive unclassified information as well as classified information.

Supplemental 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. Related control: SC-13.

A PDS provides physical protection for communications lines and can also provide need-to-know isolation.

4.21.19.2   SC-8(2) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE / POST TRANSMISSION HANDLING
Control: The IS maintains the confidentiality and integrity of information during preparation for transmission and during reception.

Supplemental 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.
Related control: AU-10.

4.21.19.3   SC-8(3) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS

Control: The IS implements cryptographic mechanisms to protect message externals unless otherwise protected by alternative physical or logical safeguards. Message externals include, for example, message headers/routing information.

Supplemental Guidance: This control enhancement addresses protection against unauthorized disclosure of information. Message externals include, for example, message headers/routing information. This control enhancement prevents the exploitation of message externals and applies to both internal and external networks or links that may be visible to individuals who are not authorized users.

Header/routing information is sometimes transmitted unencrypted because the information is not properly identified by organizations as having significant value or because encrypting the information can result in lower network performance and/or higher costs. Alternative physical safeguards include, for example, protected distribution systems. Related controls: SC-12, SC-13.

4.21.19.4   SC-8(4) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL / RANDOMIZE COMMUNICATIONS

Control: The IS implements cryptographic mechanisms to conceal or randomize communications patterns unless otherwise protected by alternative physical or logical safeguards. Communication patterns include, for example, frequency, periods, amount, and predictability. Changes to communications patterns can reveal information having intelligence value especially when combined with other available information related to missions/business functions supported by organizational information systems.

Supplemental Guidance: This control enhancement addresses protection against unauthorized disclosure of information. Communication patterns include, for example, frequency, periods, amount, and predictability. Changes to communications patterns can reveal information having intelligence value especially when combined with other available information related to missions/business functions supported by organizational information systems. This control enhancement prevents the derivation of intelligence based on communications patterns and applies to both internal and external networks or links that may be visible to individuals who are not authorized users. Encrypting the links and transmitting in continuous, fixed/random patterns prevents the derivation of intelligence from the system communications patterns. Alternative physical safeguards include, for example, protected distribution systems. Related controls: SC-12, SC-13. References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113; CNSS Policy 15; NSTISSI No. 7003.

4.21.20 SC-10 NETWORK DISCONNECT

Control: The IS terminates the network connection associated with a communications session at the end of the session or after no more than one hour of inactivity.

Supplemental 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.

Control Enhancements: None. References: None.

4.21.21 SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the IS in accordance with NSA-approved key management technology and processes.

Supplemental 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. Related controls: SC-13, SC-17.

Cryptographic keys include, but are not limited to those associated with bulk encryptors (e.g. NSA-provided cryptographic equipment), PKI, and FIPS 140-2 approved encryption modules, and may be implemented via either hardware or software. In addition, organizations shall maintain availability of information, via key escrow, in the event of the loss of cryptographic keys.

Control Enhancements:

4.21.21.1   SC-12(2) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS

Control: The organization produces, controls, and distributes symmetric keys using NSA-approved key management technology and processes.

4.21.21.2   SC-12(3) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS

Control: The organization produces, controls, and distributes asymmetric keys using NSA-approved key management technology and processes.

4.21.22 SC-13 CRYPTOGRAPHIC PROTECTION

Control: The IS implements using NSA-approved cryptography for protecting classified information from access by personnel who lack the necessary security clearance in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, and standards. To protect classified information organizations shall employ NSA-approved cryptography.

Cryptography shall also be used to protect information that must be separated from individuals who have the necessary clearances, but lack the necessary access approvals.

Supplemental 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 FIPS-validated 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). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

To protect unclassified information, organizations shall employ, at a minimum, FIPS-validated cryptography. This does not include U//HVSACO. To protect classified information and U//HVSACO, organizations shall employ NSA-approved cryptography. Cryptography shall also be used to protect information that must be separated from individuals who have the necessary clearances, but lack the necessary access approvals.

For information systems with an integrity impact level of moderate or high, FIPS-validated (e.g., FIPS 140-2) or NSA-approved cryptography shall be used, as appropriate, to implement digital signatures. This capability may be provided via either hardware or software.

4.21.23 SC-15 COLLABORATIVE COMPUTING DEVICES
Control: The information system:
    a. Prohibits remote activation of collaborative computing devices with no exceptions; and
    b. Provides an explicit indication of use to users physically present at the devices.

Supplemental 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. Related control: AC-21.

Control Enhancements:
4.21.23.1   SC-15(3) COLLABORATIVE COMPUTING DEVICES | DISABLING / REMOVAL IN SECURE WORK AREAS
Control: The organization disables or removes collaborative computing devices from organizationally-identified IS or IS components in specified secure work areas.

Supplemental Guidance: Failing to disable or remove collaborative computing devices from information systems or information system components can result in subsequent compromises of organizational information including, for example, eavesdropping on conversations.

4.21.24 SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES
Control: The organization issues public key certificates under the organizationally-defined certificate policy or obtains public key certificates from an approved service provider. This requirement addresses certificates with visibility external to the information system and certificates related to internal system operations.

Supplemental 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. Related control: SC-12.

Control Enhancements: None.
References: OMB Memorandum 05-24; NIST Special Publications 800-32, 800-63.
4.21.25 SC-18 MOBILE CODE
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.

Supplemental 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. Related controls: AU-2, AU-12, CM-2, CM-6, SI-3.

Mobile code technology is assigned to one of three risk categories:
    a. **Category 1 (High Risk):** These mobile code technologies provide broad functionality, allowing unmediated access to workstation, host, and remote system services and resources. Category 1 mobile code technologies have known security vulnerabilities with few or no countermeasures once they begin executing. They pose a severe threat to operations, and the high risk associated with their use outweighs almost all possible benefits.
    b. **Category 2 (Medium Risk):** These mobile code technologies have full functionality, allowing mediated or controlled access to workstation, host, and remote system services and resources. They also have known fine-grained, periodic, or continuous countermeasures or safeguards against security exploits. Category 2 technologies pose a moderate threat to information systems; when combined with prudent countermeasures against malicious code and exploitation, their use can afford benefits that generally outweigh the risks.
    c. **Category 3 (Low Risk):** These mobile code technologies provide limited functionality with no capability for unmediated access to workstation, host, and remote system resources and services, and they have fine-grained, periodic, or continuous security safeguards against security exploits. Category 3 technologies are of limited risk to systems. When combined with vigilance comparable to that required to keep any software system configured to resist known exploits, the use of Category 3 technologies affords benefits that generally outweigh the risks.
    d. Organizations shall comply with mobile code requirements, usage restrictions, and implementation guidance for acceptable mobile code and mobile code technologies as follows [SC-18.a and .b]:
    e. Emerging mobile code technologies, that have not undergone a risk assessment and been

assigned to a Risk Category by the AO, shall not be used.

f. Category 1 mobile code shall be signed by a trusted Certificate Authority. Use of unsigned Category 1 mobile code is prohibited. Use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.

g. Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.

h. Category 2 mobile code which does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., JWICS, SIPRNet, SSL connection, S/MIME) or when signed with an approved certificate.

i. Category 3 mobile code may be used.

Control Enhancements:

4.21.25.1   SC-18(1) MOBILE CODE | IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS

Control: The IS identifies unacceptable mobile code and takes corrective action. Corrective actions when unauthorized mobile code is detected include, for example, blocking, quarantine, or alerting the SA. Disallowed transfers include, for example, sending word processing files with embedded macros.

Supplemental Guidance: Corrective actions when unacceptable mobile code is detected include, for example, blocking, quarantine, or alerting administrators. Blocking includes, for example, preventing transmission of word processing files with embedded macros when such macros have been defined to be unacceptable mobile code.

4.21.25.2   SC-18(2) MOBILE CODE | ACQUISITION / DEVELOPMENT / USE

Control: The organization ensures that the acquisition, development and use of mobile code to be deployed in the information system meets mobile code requirements, usage restrictions, and implementation guidance for acceptable mobile code and mobile code technologies as follows:

a. Category 1 mobile code shall be signed by a trusted Certificate Authority. Use of unsigned Category 1 mobile code is prohibited. Use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.

b. Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used. Category 2 mobile code which does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., JWICS, SIPRNet, SSL connection, S/MIME) or when signed with an approved code signing certificate.

c. Category 3 mobile code may be used.

4.21.25.3   SC-18(3) MOBILE CODE | PREVENT DOWNLOADING / EXECUTION

The IS prevents the download and execution of prohibited mobile code.

4.21.25.4   SC-18(4) MOBILE CODE | PREVENT AUTOMATIC EXECUTION

The IS prevents the automatic execution of prohibited mobile code prior to executing the code.

Supplemental Guidance: Actions enforced before executing mobile code, include, for example, prompting users prior to opening electronic mail attachments. Preventing automatic execution of

mobile code includes, for example, disabling auto execute features on information system components employing portable storage devices such as CDs, DVDs, and USB devices.

4.21.26 SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization:

    a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the IS if used maliciously; and

    b. Authorizes monitors and controls the use of VoIP within the IS.

Organizations shall ensure VoIP technologies are implemented with AO and approval. The organization shall further ensure:

    a. VoIP telephone instruments shall have a "Consent to Monitor" label (e.g. DD Form 2056) or banner and an appropriate classification label or banner.

    b. VoIP telephone instruments must be used in such a way to ensure no unintended conversations are picked up and transmitted outside the facility. This may include use in an enclosed office, or ensuring no other higher classified discussions occur in the area when the VoIP telephone is in use.

Supplemental Guidance: Related controls: CM-6, SC-7, SC-15.

Control Enhancements: None.
References: NIST Special Publication 800-58.

4.21.27 SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: A Domain Name System (DNS) server is an example of an information system that provides name/address resolution service. 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.

Supplemental 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, 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. Related controls: Audit and Accountability (AU)-10, SC-8, SC-12, SC-13, SC-21, SC-22.

A Domain Name System (DNS) server is an example of an information system that provides name/address resolution service.

An example is indication of the security status of child subspaces through the use of delegation signer (DS) resource records in the DNS.

4.21.28 SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

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.

Supplemental 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. Related controls: SC-20, SC-22.

4.21.29 SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

Control: The IS that collectively provide name/address resolution service for an organization shall be fault-tolerant and implement internal/external role separation.

Supplemental Guidance: Information systems that provide name and address resolution services include, for example, 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). Related controls: SC-2, SC-20, SC-21, SC-24.

Control Enhancements: None.
References: NIST Special Publication 800-81.
4.21.30 SC-23 SESSION AUTHENTICITY

Control: The IS protects the authenticity of communications sessions. 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.

Supplemental 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. Related controls: SC-8, SC-10, SC-11.

Control Enhancements:
4.21.30.1   SC-23(1) SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT

The information system invalidates session identifiers upon user logout or other session termination.

Supplemental Guidance: This control enhancement curtails the ability of adversaries from capturing and continuing to employ previously valid session IDs.

4.21.30.2   SC-23(3) SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION

Control: The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.

Supplemental Guidance: This control enhancement curtails the ability of adversaries from reusing previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers helps to protect against brute-force attacks to determine future session identifiers. Related control: SC-13.

4.21.30.3   SC-23(5) SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES

Control: The information system only allows the use of defined certificate authorities for verification of the establishment of protected sessions.

Supplemental Guidance: Reliance on certificate authorities (CAs) for the establishment of secure sessions includes, for example, the use of Secure Socket Layer (SSL) and/or TLS certificates. These certificates, after verification by the respective certificate authorities, facilitate the establishment of protected sessions between web clients and web servers. Related control: SC-13.

References: NIST Special Publications 800-52, 800-77, 800-95.

4.21.31 SC-28 PROTECTION OF INFORMATION AT REST

Control: Information at rest refers to the state of information when it is located on a non-volatile device (e.g., hard drive, tapes) within an information system. Laptop hard drives must be encrypted using either Bit locker or other AO-approved encryption technology and must be labeled with "authorized/not authorized for travel" and "compliant with DAR policy." Information systems shall protect the confidentiality and integrity of information at rest.

Supplemental 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.
Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.

Control Enhancements:
4.21.31.1   SC-28(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION
Control: The IS implements DoD/NSA-approved cryptographic mechanisms to prevent unauthorized disclosure and modification of data at rest, to include mobile devices, CDs and other removable media (e.g., USB hard drives).

Supplemental Guidance: Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage and also to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices).

Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions. Related controls: AC-19, SC-12.

In addition, all portable media originating from an IS which has a high or moderate confidentiality rating shall be encrypted using either NSA-approved, or FIPS 140-2 compliant products, see [MP-5(4)].

4.21.32 SC-38 OPERATIONS SECURITY
Control: The organization employs OPSEC safeguards to protect key organizational information throughout the system development life cycle.

Supplemental Guidance: Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps:
    a. Identification of critical information (e.g., the security categorization process);
    b. Analysis of threats;
    c. Assessment of risks; and
    d. The application of appropriate countermeasures.

OPSEC safeguards are applied to both organizational information systems and the environments in which those systems operate. OPSEC safeguards help to protect the confidentiality of key information including, for example, limiting the sharing of information with suppliers and potential suppliers of information system components, information technology products and services, and with other non-organizational elements and individuals. Information critical to mission/business success includes, for example, user identities, element uses, suppliers, supply

chain processes, functional and security requirements, system design specifications, testing protocols, and security control implementation details. Related controls: RA-2, RA-5, SA-12.

Control Enhancements: None. References: None.
4.21.33 SC-39 PROCESS ISOLATION

Control: The IS maintains a separate execution domain for each executing process.

Supplemental 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. Related controls: AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3.

Use of a modern operating system meets this control for most systems.

4.21.34 SC-42 SENSOR CAPABILITY AND DATA

Control: The information system:
    a. Prohibits the remote activation of environmental sensing capabilities unless determined to be essential for mission execution; and
    b. Provides an explicit indication of sensor use.

This control often applies to types of information systems or system components characterized as mobile devices, for example, smart phones, tablets, and E-readers. These systems often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include, for example, cameras, microphones, Global Positioning System (GPS) mechanisms, and accelerometers.

Supplemental Guidance: This control often applies to types of information systems or system components characterized as mobile devices, for example, smart phones, tablets, and E-readers. These systems often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include, for example, cameras, microphones, GPS mechanisms, and accelerometers. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the specific movements of an individual.

Control Enhancements:
4.21.34.1   SC-42(3) SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES

Control: The organization prohibits the use of devices possessing environmental sensing capabilities within facilities.

Supplemental Guidance: For example, organizations may prohibit individuals from bringing cell phones or digital cameras into certain facilities or specific controlled areas within facilities where classified information is stored or sensitive conversations are taking place.

References: None.

4.22   SYSTEM AND INFORMATION INTEGRITY

4.22.1 SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization:
   a. Develops, documents, and disseminates to **all 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 the current:
      (1) System and information integrity policy **at least annually**; and
      (2) System and information integrity procedures **at least annually**.

Supplemental 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. Related control: PM-9.

Policy and procedures related to system and information integrity are defined in the remainder of this section.

Control Enhancements: None. References: NIST Special Publications 800-12, 800-100.

4.22.2 SI-2   FLAW REMEDIATION

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 within **thirty (30) days** of the release of the updates; and
   d. Incorporates flaw remediation into the organizational configuration management process.

Flaw remediation refers to software patch management. Patch management is the systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions.

Organizations shall:
   a. Ensure system/network administrators routinely review vendor sites, bulletins, and notifications and proactively update information systems with fixes, patches, definitions, service packs, or implementation of vulnerability mitigation strategies with ISSM approval; and
   b. Employ automated patch management tools on all components to the maximum extent

supported by available tools to facilitate flaw remediation.

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). 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, for example, when implementing simple anti-virus signature updates.

Supplemental 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, hot fixes, and anti-virus signatures. 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 CWE or 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 f o r 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, for example, when implementing simple anti-virus s i g n a t u r e updates.

Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.

Control Enhancements:
4.22.2.1 SI-2(1) FLAW REMEDIATION | CENTRAL MANAGEMENT
Control: The organization centrally manages the flaw remediation process.

Supplemental 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.

4.22.2.2   SI-2(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

Control: The organization employs automated mechanisms **at least once a quarter** to determine the state of information system components with regard to flaw remediation. Supplemental Guidance: Related controls: CM-6, SI-4.

4.22.2.3 SI-2(3) FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS

Control: The organization:

a. Measures the time between flaw identification and flaw remediation; comparing with a local historical development of benchmarks, if available.

Supplemental Guidance: This control enhancement requires organizations to determine the current time it takes on the average to correct information system flaws after such flaws have been identified, and subsequently establish organizational benchmarks (i.e., time frames) for taking corrective actions.

Benchmarks can be established by type of flaw and/or severity of the potential vulnerability if the flaw can be exploited.

Historical benchmarks, if available, can be used as a reference point for comparison.

4.22.2.4 SI-2(6) FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE

Control: The organization removes previous versions of software and/or firmware components after updated versions have been installed.

Supplemental Guidance: Previous versions of software and/or firmware components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software and/or firmware automatically from the information system. References: NIST Special Publications 800-40, 800-128.

4.22.3 SI-3   MALICIOUS CODE PROTECTION

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 organizational configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
   (1) Perform periodic scans of the information system **at least weekly** and real-time scans of files from external sources at **endpoints and 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 an alert to the system administrator** in response to malicious code detection.
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.

Supplemental 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. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

In reference to SI-3.b, malicious code protection mechanisms shall be updated, at a minimum, every 30 days.

Control Enhancements:
4.22.3.1 SI-3(1) MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT
Control: The organization centrally manages malicious code protection mechanisms, e.g. client/server antivirus model, records of malicious code protection updates; information system configuration settings and associated documentation.

Supplemental 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. Related controls: AU-2, SI-8.

Central management of malicious code protection includes client/server antivirus model, records of malicious code protection updates; information system configuration settings and associated documentation.

4.22.3.2 SI-3(2) MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES
Control: The information system automatically updates malicious code protection mechanisms (including signature definitions), i.e. after updates are installed to the server.

Page 213

Supplemental 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. Related control: SI-8.

Information systems shall automatically update malicious code protection mechanisms (including signature definitions), i.e., after updates are installed to the server.

4.22.3.3 SI-3(10) MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS

Control: The organization:

    a. Employs specific tools and techniques to analyze the characteristics and behavior of malicious code; and

    b. Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes.

Supplemental Guidance: The application of selected malicious code analysis tools and techniques provides organizations with a more in-depth understanding of adversary tradecrTD/AFT(i.e., tactics, techniques, and procedures) and the functionality and purpose of specific instances of malicious code. Understanding the characteristics of malicious code facilitates more effective organizational responses to current and future threats. Organizations can conduct malicious code analyses by using reverse engineering techniques or by monitoring the behavior of executing code. References: NIST Special Publication 800-83.

4.22.4 SI-4   INFORMATION SYSTEM MONITORING

Control: The organization

    a. Monitors the information system to detect:

        (1) Attacks and indicators of potential attacks in accordance with the Service or Activity policy; and

        (2) Unauthorized local, network, and remote connections;

    b. Identifies unauthorized use of the information system through **User Activity Monitoring tools, such as InTrust;**

    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 information as needed to designated personnel.

Supplemental 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. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

Control Enhancements:
4.22.4.1 SI-4(1) INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM
Control: The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

4.22.4.2 SI-4(2) INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS
Control: The organization employs automated tools to support near real-time analysis of events. Supplemental 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.

4.22.4.3 SI-4(4) INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC
Control: The information system monitors inbound and outbound communications traffic **continuously** for unusual or unauthorized activities or conditions.

Supplemental 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.

4.22.4.4   SI-4(5) INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS

Control: The information system alerts ISSM/ISSO when the following indications of compromise or potential compromise occur: audit record deletion or modification, alerts from malicious code detection mechanisms, intrusion detection or prevention mechanisms, boundary protection mechanisms such as firewalls, gateways, and routers.

Supplemental 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. Related controls: AU-5, PE-6.

System alerts may be sent to the system administrator, ISSO, ISSM for indicators related to audit records, alerts from malicious code detection mechanisms, intrusion detection or prevention mechanisms, boundary protection mechanisms such as firewalls, gateways, and routers.

4.22.4.5 SI-4(10) INFORMATION SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS

Control: The organization makes provisions so that Program-related encrypted communications traffic is visible to deployed IS monitoring tools.

Supplemental Guidance: Organizations balance the potentially conflicting needs for encrypting communications traffic and for having insight into such traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of communications traffic is paramount; for others, mission-assurance is of greater concern. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.

4.22.4.6 SI-4(11) INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES

Control: The organization analyzes outbound communications traffic at the external boundary of the IS and selected subnetworks/subsystems to discover anomalies. Anomalies within organizational information systems include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.

Supplemental Guidance: Anomalies within organizational information systems include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.

4.22.4.7 SI-4(12) INFORMATION SYSTEM MONITORING | AUTOMATED ALERTS

Control: The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: **at a minimum including unauthorized access attempts, unauthorized system usage**. E-mail or security

dashboard alerts meet the intent of this control and can be set up to summarize user unauthorized access attempts to files or authentication failures.

Supplemental Guidance: This control enhancement focuses on the security alerts generated by organizations and transmitted using automated means. In contrast to the alerts generated by information systems in SI-4(5), which tend to focus on information sources internal to the systems (e.g., audit records), the sources of information for this enhancement can include other entities as well (e.g., suspicious activity reports, reports on potential insider threats). Related controls: AC-18, IA-3.

4.22.4.8 SI-4(14) INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION

Control: The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

Supplemental Guidance: Wireless signals may radiate beyond the confines of organization-controlled facilities. Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. Scans are not limited to those areas within facilities containing information systems, but also include areas outside of facilities as needed, to verify that unauthorized wireless access points are not connected to the systems. Related controls: AC-18, IA-3.

Organizations should proactively monitor for unauthorized wireless connections, including scanning for unauthorized wireless access points at least quarterly**.**

Unauthorized wireless devices require reporting and response in accordance with the organization/system incident response plan.

4.22.4.9 SI-4(15) INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS

Control: The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

Supplemental Guidance: Related control: AC-18.

4.22.4.10   SI-4(16) INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION

Control: To the extent possible, the organization correlates information from monitoring tools employed throughout the information system to achieve organization-wide situational awareness. This control supports insider threat mitigation.

Supplemental Guidance: Correlating information from different monitoring tools can provide a more comprehensive view of information system activity. The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns. Understanding the capabilities/limitations of diverse monitoring tools and how to maximize the utility of information generated by those tools can help organizations to build, operate, and maintain effective monitoring programs. Related control: AU-6.

4.22.4.11   SI-4(19) INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK

Control: The organization implements additional monitoring measures of individuals who have been identified by organization and/or other authorized sources as posing an increased level of risk. Indications of increased risk from individuals can be obtained from a variety of sources including, for example, human resource records, intelligence agencies, law enforcement organizations, and/or other credible sources. The monitoring of individuals is closely coordinated with management, legal, security, and human resources officials within organizations conducting such monitoring and complies with federal legislation, Executive Orders, policies, directives, regulations, and standards.

Supplemental Guidance: Indications of increased risk from individuals can be obtained from a variety of sources including, for example, human resource records, intelligence agencies, law enforcement organizations, and/or other credible sources. The monitoring of individuals is closely coordinated with management, legal, security, and human resources officials within organizations conducting such monitoring and complies with federal legislation, Executive Orders, policies, directives, regulations, and standards.

4.22.4.12   SI-4(20) INFORMATION SYSTEM MONITORING | PRIVILEGED USER

Control: The organization implements additional monitoring or privileged users. Additional monitoring may be instituted as part of a new-user policy, upon notice of personnel termination (e.g., user gives two weeks' notice), or the result of incident response. This control may be implemented and defined at the time of incident.

Example: Following an incident related to incorrect marking, the GSSO/institutes probationary period of 30 days during which time a designated security person reviews all documents produced by the individual.

Implementation of AU-2 controls may address this security control. Identify additional monitoring activities required by the AO.

4.22.4.13   SI-4(21) INFORMATION SYSTEM MONITORING | PROBATIONARY PERIODS

Control: The organization implements additional monitoring of individuals during probationary periods.

Additional monitoring may be instituted as part of a new-user policy, upon notice of personnel termination (e.g., user gives two weeks' notice), or the result of incident response. This control may be implemented and defined at the time of incident.

4.22.4.14   SI-4(22) INFORMATION SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES

Control: Information system detects network services that have not been authorized or approved by defined authorized or approval processes and audits and/or alerts the ISSM/ISSO.

Supplemental Guidance: Unauthorized or unapproved network services include, for example, services in service-oriented architectures that lack organizational verification or validation and therefore may be unreliable or serve as malicious rogues for valid services. Related controls: AC-6, CM-7, SA-5, SA-9.

4.22.4.15   SI-4(23) INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES

Control: The organization implements host-based monitoring at identified IS components. This includes monitoring, for example, of I/O and endpoint services.

Supplemental Guidance: Information system components where host-based monitoring can be implemented include, for example, servers, workstations, and mobile devices. Organizations consider employing host-based monitoring mechanisms from multiple information technology product developers.

This includes monitoring, for example, I/O and endpoint services, reference [AC-6(1)].

4.22.5 SI-5   SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control: The organization:

a. Receives information system security alerts, advisories, and directives from includes, but is not limited to, the Joint Task Force Global Network Operations, DHS US-CERT, System Administration, Networking, and Security (SANS) Internet Storm Center (ISC) and USCYBERCOM on an ongoing basis; This includes, but is not limited to, the **Department of Homeland Security (DHS) US-CERT, SANS ISC and USCYBERCOM;**

b. Generates internal security alerts, advisories, and directives as deemed necessary;

c. Disseminates security alerts, advisories, and directives to: **ISOs, ISSM/ISSOs, system administrators, and security personnel, as appropriate**; and

d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Supplemental 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. Related control: SI-2.

A variety of sites are available that provide warnings of system vulnerabilities or ongoing attacks. Additional sources of alerts and advisories which may be monitored include:

a. DHS US Computer Emergency Readiness Team.

b. Military service computer security incident response teams (CSIRTs) (i.e., Air Force Network Operations and Security Center Network Security Division (AFNOSC NSD), Army CERT – Computer Network Operations (ACERT-CNO), Navy Cyber Defense Operations Command (NCDOC), and Marine Corps Network Operations and Security Command (MCNOSC)).

c. Advisories from the IC Security Coordination Center (IC-SCC) such as Intelligence Community Vulnerability Alerts (ICVA) and Intelligence Community Vulnerability Management (ICVM) releases.

d. IAVAs and IAVBs maintained by USCYBERCOM and Defense Information Systems Agency (DISA).

4.22.5.1   SI-7(14) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE

The organization:
   a. Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and
   b. Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/firmware and open source software. Organizations assess software products without accompanying source code from sources with limited or no warranty for potential security impacts. The assessments address the fact that these types of software products may be very difficult to review, repair, or extend, given that organizations, in most cases, do not have access to the original source code, and there may be no owners who could make such repairs on behalf of organizations. Related control: SA-5.

4.22.6 SI-10 INFORMATION INPUT VALIDATION

Control: The information system checks the validity of all inputs to web/application servers, database servers, and any system or application input that might receive a crafted exploit toward executing some code or buffer overflow.

Supplemental 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.

Not all operating systems / applications provide input validation. The system configuration documentation will address what inputs are checked and what input format and content is acceptable.

4.22.7 SI-11 ERROR HANDLING

Control: The information system:
   a. Generates error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries; and
   b. Reveals error messages only to authorized personnel.

Supplemental 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. Related controls: AU-2, AU-3, SC-31.

Systems should be configured to reduce access to system errors and logs that could reveal sensitive or security related information to adversaries to those personnel identified as privileged users with a requirement to access such information.

Control Enhancements: None. References: None.

4.22.8 SI-12 INFORMATION HANDLING AND RETENTION

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.

ASPD provides guidance for information retention.

Supplemental 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. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4.

Control Enhancements: None. References: None.

4.23   PROGRAM MANAGEMENT

4.23.1 PM-1 INFORMATION SECURITY PROGRAM PLAN

The SSP can function as the Security Plan for ISSMs. 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 **at least annually**;
    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.

Supplemental 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. Related control: PM-8.

Policy and procedures related to program management controls are defined in the remainder of this section with the goal to develop and disseminate an organization-wide information security program.

Control Enhancements: None. References: None.
4.23.2 PM-2 SENIOR INFORMATION SECURITY OFFICER *(Removed from DSS Baseline)*

Control Enhancements: None. References: None.
4.23.3 PM-3 INFORMATION SECURITY RESOURCES
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.

Supplemental 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. Related controls: PM-4, SA-2.

Control Enhancements: None.
References: NIST Special Publication 800-65.

4.23.4 PM-4 PLAN OF ACTION AND MILESTONES PROCESS

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 reporting requirements.

    b. Reviews Plans of Action and Milestones (POA&M) for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

DSS requires ISSM to monitor POA&Ms and provide updates to the DSS by submitting an administrative update for the IS (M)SSP. Status updates should be submitted at least quarterly.

Supplemental 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 vulnerabilities from security control assessments and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. Related control: CA-5.

Plans of Action and Milestones (POA&Ms) developed for authorization packages for authorization [CA-5] of systems within the organization must be reviewed from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization.

Control Enhancements: None.
References: OMB Memorandum 02-01; NIST Special Publication 800-37.

4.23.5 PM-5 INFORMATION SYSTEM INVENTORY

Control: The organization develops and maintains an inventory of its information systems. Each ISSM is required to maintain an inventory of information systems under its purview; ensuring information related to the number, size, and mission information system is maintained.

Supplemental 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.

The SSP captures external information systems in proximity to the system under assessment, i.e., within the accredited area. The organization's information security program maintains an inventory of information systems under its purview, ensuring information related to the number, size, and mission of information systems is maintained.

Control Enhancements: None. References: Web: http://www.omb.gov.

4.23.6   PM-6   INFORMATION SECURITY MEASURES OF PERFORMANCE

Control: The organization develops, monitors, and reports on the results of information security measures of performance, e.g. metrics. See NIST SP 800-55, Performance Measurement Guide for Information Security, for metrics examples.

Information security measures monitor the accomplishment of goals and objectives by quantifying the implementation, efficiency, and effectiveness of security controls; analyzing the adequacy of information security program activities; identifying possible improvement actions.

a. Number of employees who received annual security awareness training;
b. Percent of information systems with approved ATOs;
c. Number of privileged users;
d. Number of low and high risk Data Transfer Agents; and
e. Other measurements as required by the AO in accordance with the CSAs Assessment and Authorization Manual.

Supplemental 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.

As stated in NIST SP 800-55, *Performance Measurement Guide for Information Security,* "Information security measures monitor the accomplishment of goals and objectives by quantifying the implementation, efficiency, and effectiveness of security controls; analyzing the adequacy of information security program activities; and identifying possible improvement actions."

Information security measurements are frequently captured as a percentage, e.g.:

a. Percent of employees who received annual security awareness training;
b. Percent of employees who received annual information assurance awareness training; or
c. Percent of information systems with approved system security plans.

Additional guidance on capturing measures of performance and suggested sources for items that should be measured may be found in NIST SP 800-55.

Control Enhancements: None.
References: NIST Special Publication 800-55.

4.23.7 PM-7   ENTERPRISE ARCHITECTURE

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 and ensures security considerations are addressed by the organization early in the system development life cycle and that the requirements and controls assigned are directly and explicitly related to the organization's mission/business processes.

Supplemental 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, 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. Related controls: PL-2, PL-8, PM-11, RA-2, SA-3.

Data collected in support of the Information Security Program, primarily the security requirements and controls required for security authorization [CA-6] and life cycle support [SA-3] are integrated into the organization's enterprise architecture to ensure security considerations are addressed by the organization early in the system development life cycle and that the requirements and controls assigned are directly and explicitly related to the organization's mission/business processes.

Control Enhancements: None.
References: NIST Special Publication 800-39.
4.23.8 PM-8   CRITICAL INFRASTRUCTURE PLAN
Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Supplemental 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. Related controls: PM-1, PM-9, PM-11, RA-3.

Identifying and documenting critical infrastructure and key resources provides the organization with the fundamental understanding of what assets need protection, at what level, ensures focus on the mission/business objectives, and supports contingency planning [CP-2].

Control Enhancements: None.
References: HSPD 7; National Infrastructure Protection Plan.
4.23.9 PM-9   RISK MANAGEMENT STRATEGY
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 **at least annually** or as required and to address organizational changes.

The risk management strategy at the Program Level incorporates the risk assessment results from the risk assessment reports provided for the security authorization of the information systems (RA-3), as well as other sources internal and external to the organization resulting in a comprehensive risk management strategy.

Supplemental 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. Related control: RA-3.

Control Enhancements: None.
References: NIST Special Publications 800-30, 800-39.
4.23.10PM-10 SECURITY AUTHORIZATION PROCESS
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 (i.e., ISSM/ISSO); and
   c. Fully integrates the security authorization processes into an organization-wide risk management program.

The organization must implement the Risk Management Framework and incorporate the processes required for security authorization in accordance with the requirements of the NISPOM and CSA's Assessment and Authorization Manual.

Supplemental 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. Related control: CA-6.

Control Enhancements: None.
References: NIST Special Publications 800-37, 800-39.
4.23.11 PM-11 MISSION/BUSINESS PROCESS DEFINITION
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.

Supplemental 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. Related controls: PM-7, PM-8, RA-2.

Identifying and defining the organization's mission/business processes is required in order to identify critical infrastructures and key resources, and in turn the organization's operations, assets, and individuals that may be at risk, which determines the information protection needs based on the level of adverse impact if a compromise of information occurs. Security categorization describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be compromised through a loss of confidentiality, integrity, or availability and results in a potential impact level of low, moderate, or high, which indicates the set of protection needs required. Reference Section 2 of this document and [RA-2].

Control Enhancements: None.
References: FIPS Publication 199; NIST Special Publication 800-60.
4.23.12 PM-12 INSIDER THREAT PROGRAM
Control: The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team (i.e., ISSM, PM, etc.).

The organization required to comply with the requirements of the NISP Insider Threat Program. Supplemental 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 government-owned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis, and conduct self-assessments of department/agency insider threat posture.

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. Related controls: AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4, PM-1, PM-14.

An Insider Threat Program is system independent at the top level. At the system level, the following controls (not all-inclusive) can be linked to Insider Threat Program implementation: AC-2(12), AC-2(13), AC-3(2), AC-5, AC-6, AC-6(7), AC-6(8), AC-6(9), AC-6(10), AT-2(2), AU-6, AU-6(5), AU-6(8), AU-12, AU-16, CM-5, CM-8(3), IA-2, IR-4, IR-10, MP-2, MP-7, PE-3, PS-3, PS-4, SI-4, and SC-28.

Control Enhancements: None. References: Executive Order 13587.
4.23.13 PM-13 INFORMATION SECURITY WORKFORCE
Control: The organization establishes an information security workforce development and improvement program.

Appropriate staff is required to establish and maintain an adequate information security workforce certified in accordance with the requirements of DOD 8570.01-M if imposed by contract.

Supplemental 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. Related controls: AT-2, AT-3.

Examples: Organizations must ensure that individuals responsible for performing maintenance on accounts (e.g., account manager) have direction on who is able to make decisions about the different types of accounts directed in AC-2.

Control Enhancements: None. References: None.
4.23.14 PM-14   TESTING, TRAINING, AND MONITORING
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.
   c. Each Organization required to consider OPSEC as it pertains to their information security if contractually imposed.

Supplemental 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. Related controls: AT-3, CA-7, CP-4, IR-3, SI-4.

Control Enhancements: None.
References: NIST Special Publications 800-16, 800-37, 800-53A, 800-137.
4.23.15 PM-15 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS
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.

The organization must provide oversight for the security testing, training, and monitoring activities conducted within their facility and ensure that those activities are coordinated.

Supplemental 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. Related control: SI-5.

A number of venues are available to organizational personnel to facilitate ongoing security education, awareness and training. These include, for example:
   a. System Administration;
   b. Networking; and
   c. SANS Institute.

IA and CND personnel will maintain contact with sponsoring agency/organization's IA office to stay up to date with the latest security policies, practices, techniques, and technologies. This information will be further disseminated as required.

Control Enhancements: None. References: None.
4.23.16 PM-16 THREAT AWARENESS PROGRAM
Control: The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

The organization must create and follow procedures to release information below the accredited level of the system. A record must be maintained and the trusted download agent must be trained. A comprehensive review should be completed by knowledgeable users.

Supplemental Guidance: Because of the constantly changing and increasing sophistication of adversaries, especially the 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 s p e c i a l agreements and protection, or less sensitive and freely shared. Related controls: PM-12, PM-16.
Control Enhancements: None. References: None.

AP	Authority and Purpose
AR	Accountability, Audit, and Risk
DI	Data Quality and Integrity
DM	Data Minimization and Retention
IP	Individual Participation and
SE	Security
TR	Transparency
UL	Use Limitation

Privacy Control Families and Identifiers

Supplemental Guidance: When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the Senior Agency Official for Privacy (SAOP)/CPO and legal counsel, that there is a close nexus between the general authorizations. 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. Related controls: AR-2, AR-4, AR-5, DM-1, DM-2, TR-1, TR-2, UL-1, UL-2.

Control Enhancements: None. References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)(A)-(B); Sections 208(b), (c), E-Government Act o f 2002 (P.L. 107-347).

APPENDIX B: REFERENCES

- Executive Order 12829, *"National Industrial Security Program,"* January 6, 1993
- Executive Order 13526, *Classified National Security Information*, December 29, 2009.
- DoD 5220.22-M, Change 2, National Industrial Security Program Operating Manual, March 28, 2013
- National Industrial Security Program Manual, Change 2, May 18, 2016
- CNSSI-1253, *Security Categorization and Control Selection for National Security Systems*, March 27, 2014
- CNSSI-4009, *National Information Assurance (IA) Glossary*, April 6, 2015
- CNSSI-7003, *Protected Distribution Systems (PDS),* September 13, 1996.
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010.
- NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, April 2013 (Updates as of January 22, 2015).
- NIST SP 800-53A, Revision 4, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans* December 2014.
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories,* Aug 2008.
- NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, August 2012.
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* September 2011.
- FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001; Change notice December 3, 2002.

APPENDIX C: ACRONYMS

A&A	Assessment and Authorization
AC	Access Control
ACAS	Assured Compliance Assessment Solution
AFT	Assured File Transfer
AI	Administrative Inquiry
AO	Authorizing Official
ATC	Authorization to Connect
ATO	Authorization to Operate
AU	Audit and Accountability
BoE	Body of Evidence
CCP	Common Control Provider
CDS	Cross Domain Solution
CI	Controlled Interface
CI	Counterintelligence
CM	Configuration Management
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COMSEC	Communications Security
CONOPS	Concept of Operations
COOP	Continuity of Operations
COTS	Commercial-off-the-Shelf
CP	Contingency Planning
CSA	Cognizant Security Agency
DATO	Denied Authorization to Operate
DCO	Device Configuration Overlay
DMZ	Demilitarized Zone
DNS	Domain Name System
DRP	Disaster Recovery Plan
DTA	Data Transfer Agent
DVD	Digital Versatile Disk
EAP	Extensible Authentication Protocol
EPL	Evaluated Products List
EPROM	Erasable PROM
FPGA	Field Programmable Gate Array
FRD	Formerly Restricted Data
FSO	Facility Security Officer
FTP	File Transfer Protocol
GCA	Government Contracting Agency
GIG	Global Information Grid
GOTS	Government off-the-shelf
GMT	Greenwich Mean Time
HTTP	Hyper Text Transfer Protocol
I&A	Identification and Authentication
IATO	Interim Approval to Operate
I/O	Input/Output (e.g. I/O Port)
IA	Identification and Authentication
IA	Information Assurance

IDS	Intrusion Detection System
IO	Information Owner
IP	Internet Protocol
IR	Incident Response
IR	Infrared
IS	Information System
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
ISO	Information System Owner
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISSP	Information System Security Professional (New term: SCA)
IT	Information Technology
ITPSO	Insider Threat Program Senior Official
JTF	Joint Task Force
KVM	Keyboard/Video/Mouse
MA	Maintenance
MAC	Media Access Control
MP	Media Protection
MSSP	Master System Security Plan (New term: Type Authorization)
NAPA	NISP Administration and Policy Analysis
NIC	Network Interface Card
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PAN	Personal Area Network
PCL	Product Compliant List
PDA	Personal Digital Assistant
PE	Physical and Environmental Protection
PED	Portable Electronic Device
PL	Planning
PL	Protection Level (New term: Impact Level)
PM	Program Management
PM	Program Manager (aka ISO)
POA&M	Plan of Action and Milestones
POC	Point of Contact
PROM	Programmable Read-Only Memory
PS	Personnel Security
PSI	Personnel Security Investigation
PSI	Program Security Instruction
RA	Risk Assessment
RAL	Risk Acknowledgement Letter
RAM	Random Access Memory
RAR	Risk Assessment Report
RD	Restricted Data
RF	Radio Frequency
RFID	Radio Frequency Identification
RMAT	Remote Maintenance and Testing

RMF	Risk Management Framework
RO	Releasing Officer
ROM	Read Only Memory
SA	System and Services Acquisition
SCA	Security Control Assessor
SCAP	Security Content Automation Protocol (pronounced S-CAP)
SCC	SCAP Compliance Checker
SCG	Security Classification Guide
SI	System and Information Integrity
SOP	Standard Operating Procedures
SP	Special Publications
SSL	Secure Socket Layer
SSP	System Security Plan
STE	Secure Terminal Equipment
STIG	Security Technical Implementation Guide
SUSA	Single User-Standalone
SVA	Security Vulnerability Assessment
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TSCO	Top Secret Control Officer
UAC	User Account Control
UHF/VHF	Ultra High Frequency/Very High Frequency
USERID	Individual user identifier
USG	U.S. Government
VPL	Validated Products List
VPN	Virtual Private Network
VTC	Video Teleconference
VVoIP	Voice and Video Over IP
WAN	Wide Area Network
WDE	Whole Disk Encryption

Characteristics and Assumptions Stand-Alone
Extensive technical security controls are normally inappropriate and potentially expensive for standalone information systems. This overlay provides guidance on the security controls required to be implemented on standalone information systems. A stand-alone information system (IS) is a single desktop or similar component. It is not connected to any other system or LAN, has no network interface card (NIC) or protected distribution system (PDS) in place.

- The standalone overlay applies to the system if the answers to the questions below are "YES".
- Is the information system a single workstation or laptop?
- Is the information system void of any connection (wired or wireless)?
- If the answer is "NO", then use of this overlay is not applicable.
- If the information system has a single user - use the "SUSA" control set.
- If the information system has multiple users - use the "MUSA" control set.

Characteristics and Assumptions Isolated LAN Overlay
A local area network (LAN) is defined as a group of computers and network devices connected together over a relatively small geographic area. A LAN may be isolated – system boundary is completely contained to within the Facility/Building. It is not an Interconnected System.

An isolated LAN has none of the following:
- Connectivity to any other LAN
- VoIP
- Collaborative Computing

Implementation: All Overlays

- CNSSI 1253, Security Categorization and Control Selection for National Security Systems,
- NIST SP 800-53, Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations,
- All Overlays assumes a minimum baseline of MLL with the Classified Overlay. The removed controls are intended to apply a risk managed application of the CNSSI 1253 baseline controls.

Table of Overlay Security Controls
The table below contains a summary of the security control specifications as they apply to the Standalone Overlay. The symbol(s) used in the table are as follows:
- Two dashes ("--") indicates the control should not be selected.
- The letter "G" indicates there is supplemental guidance, including specific tailoring guidance if applicable, for the control.

Table 1: Security Controls for the Overlays

Ctrl Nr	Ctrl Name	SUSA	MUSA	A/V	ISOL	P2P
AC-2(1)	Account Management: Automated System Account Management	-	-	-	-	-

Ctrl Nr	Ctrl Name	SUSA	MUSA	A/V	ISOL	P2P
AC-2(2)	Account Management: Removal of Temporary or Emergency Accounts	-	-	-	-	-
AC-2(3)	Account Management: Disable Inactive Accounts	-	-	-		-
AC-2(7)	Account Management: Role Based Schemes	-				
AC-2(9)	Restrictions on use of Shared Groups / Accounts	-				
AC-2(10)	Shared / Group Account Credential Termination	-				
AC-2(12)	Account Monitoring / Atypical Usage	-				
AC-2(13)	Disable Accounts For High-Risk Individuals	-				
AC-3	Access Enforcement	-		G		
AC-3(2)	Dual Authorization	-		-		
AC-3(4)	Access Enforcement: Discretionary Access Control	-		-		
AC-6(7)	Review Of User Privileges	-				
AC-7	Unsuccessful Logon Attempts	G				
AC-10	Concurrent Session Control	-	-	-		
AC-16(7)	Consistent Attribute Interpretation	-	-	-	-	
AC-17	Remote Access	-	-	-	-	
AC-17(1)	Remote Access: Automated Monitoring/Control	-	-	-	-	
AC-17(2)	Remote Access: Protection of Confidentiality/Integrity Using Encryption	-	-	-	-	
AC-17(3)	Remote Access: Managed Access Control Points	-	-	-	-	
AC-17(4)	Remote Access: Privileged Commands/Access	-	-	-	-	
AC-17(6)	Remote Access: Protection of Information	-	-	-	-	
AC-17(9)	Disconnect / Disable Access	-	-	-	-	
AC-18(1)	Wireless Access: Authentication & Encryption	-	-	-		
AC-18(4)	Wireless Access: Restrict Configurations by Users	-	-	-		
AC-20(1)	Use of External Information Systems: Limits on Authorized Use	-	-	-		
AC-20(4)	Network Accessible Storage Devices	-	-	-		
AC-22	Publicly Accessible Content	-	-	-	-	
AC-23	Data Mining Protection	-	-	-		
AU-3(1)	Content of Audit Records: Additional	-	-	-		

Ctrl Nr	Ctrl Name	SUSA	MUSA	A/V	ISOL	P2P
	Audit Information					
AU-4(1)	Transfer To Alternate Storage	-	-	-		
AU-5	Response to Audit Processing Failures	G				
AU-6	Audit Review, Analysis, and Reporting	G				
AU-6(1)	Audit Review, Analysis and Reporting: Process Integration	-	-	-		-
AU-6(3)	Audit Review, Analysis, and Reporting: Correlate Audit Repositories					-
AU-6(4)	Audit Review, Analysis, and Reporting: Central Review and Analysis					-
AU-6(8)	Full Text Analysis Of Privilege Commands	-	-	-		
AU-7	Audit Reduction and Report Generation	-				
AU-7(1)	Audit Reduction and Report Generation: Automatic Processing	-	-	-		
AU-8(1)	Time Stamps: Synchronization with an Authoritative Time Source	-	-	-		-
AU-9(4)	Protection of Audit Information: Access by Subset of Privileged Users	-				
AU-14(3)	Remote Viewing / Listening	-	-	-	-	
AU-16	Cross-Organizational Auditing				-	
AU-16(1)	Identity Preservation				-	
AU-16(2)	Sharing of Audit Information				-	
CA-3	Information System Connections	-	-	-	-	-
CA-3(1)	Information System Connections: Unclassified National Security System Connections	-	-	-	-	
CA-3(2)	Information System Connections: Classified National Security System Connections	-	-	-	-	
CA-3(5)	Restrictions on External System Connections	-	-	-		
CA-9	Internal System Connections	-	-	-		
CM-5(5)	Access Restrictions for Change: Limit Production/Operational Privileges	-				
CM-5(6)	Access Restrictions for Change: Limit Library Privileges	-				
CM-7(2)	Least Functionality: Prevent Program Execution	-	-	-		
CM-7(3)	Least Functionality: Registration Compliance	-	-	-	-	

Ctrl Nr	Ctrl Name	SUSA	MUSA	A/V	ISOL	P2P
CM-8(2)	Automated Maintenance	-	-	-		-
CM-8(3)	Information System Component Inventory: Automated Unauthorized Component Detection	-	-	-		-
CP-7	Alternate Processing Site including CP-7(5)	-	-	-		
IA-2(1)	Identification and Authentication (Organizational Users): Network Access to Privileged Accounts	-	-	-	-	-
IA-2(2)	Identification and Authentication (Organizational Users): Network Access to Non-Privileged Accounts	-	-	-	-	-
IA-2(3)	Identification and Authentication (Organizational Users): Local Access to Privileged Accounts	-	-	-	-	
IA-2(4)	Identification and Authentication (Organizational Users): Local Access to Non-Privileged Accounts	-	-	-	-	-
IA-2(5)	Identification and Authentication (Organizational Users): Group Authentication	-				
IA-2(8)	Identification and Authentication (Organizational Users): Network Access to Privileged Accounts – Replay Resistant	-	-	-		-
IA-2(9)	Identification and Authentication (Organizational Users): Network Access to Non-Privileged Accounts – Replay Resistant	-	-	-		-
IA-2(11)	Remote Access-Separate Device	-	-	-	-	-
IA-2(12)	Acceptance of PIV Credentials	-	-	-	-	-
IA-3	Device Identification And Authentication	-	-	-		
IA-3(1)	Cryptographic Bidirectional Authentication	-	-	-		-
IA-3(3)	Device Identification and Authentication: Dynamic Address Allocation	-	-			
IA-4(4)	Identifier Management: Identify User Status	-	-	-		-
IA-5(2)	Authenticator Management: PKI-Based Authentication	-	-	-	-	-
IA-5(11)	Hardware Token-Based Authentication	-	-	-	-	
IA-5(13)	Expiration of Cached Authenticators	-	-	-		
IA-5(14)	Managing Content of PKI Trust Stores	-	-	-	-	-

Ctrl Nr	Ctrl Name	SUSA	MUSA	A/V	ISOL	P2P
IA-8	Identification and Authentication (Non-Organizational Users)	-				
IA-8(1)	Acceptance of PIV Credentials From Other Agencies	-	-	-	-	-
IA-8(2)	Acceptance of Third-Party Credentials	-	-	-	-	-
IA-8(3)	Use of FICAM-Approved Products	-	-	-	-	-
IA-8(4)	Use of FICAM-Issued Profiles	-	-	-	-	-
IR-4(1)	Automated Incident Handling Processes	G	G	G		
IR-6(1)	Incident Reporting: Automated Reporting	G	G	G		
IR-7(1)	Incident Response Assistance: Automation Support for Availability of Information	G	G	G		
IR-10	Integrated Information Security Cell	G	G	G		
MA-4	Non-Local Maintenance	-	-	-		
MA-4(3)	Non-Local Maintenance: Comparable Security/Sanitization	-	-	-		
MA-4(6)	Non-Local Maintenance: Cryptographic Protection	-	-	-		
MA-4(7)	Non-Local Maintenance: Remote Disconnect Verification	-	-	-		
PE-4	Access Control for Transmission Medium	-	-	-		
PE-17	Alternate Work Site	-	-	-		
SA-4(10)	Use of Approved PIV Products	-	-	-		-
SA-9	External Information System Services	-	-	-	-	
SA-9(1)	External Information System Services: Risk Assessment/Organizational Approvals	-	-	-	-	-
SA-9(2)	Identification of Functions/ PORTS / PROTOCOLS / SERVICES	-	-	-	-	
SC-4	Information in Shared Resources	-				
SC-4(2)	Periods Processing	G	G	G		
SC-5	Denial of Service Protection	-	-	-	-	
SC-5(1)	Denial of Service Protection: Restrict Internal Users	-	-	-	-	
SC-7	Boundary Protection includes SC-7(1) – Boundary Protection: Physically Separated Subnetworks and SC-7(2) – Boundary Protection: Public Access	-	-	-	-	-
SC-7(3)	Boundary Protection: Access Points	-	-	-	-	
SC-7(4)	Boundary Protection: External Telecommunications Services	-	-	-	-	

Ctrl Nr	Ctrl Name	SUSA	MUSA	A/V	ISOL	P2P
SC-7(5)	Boundary Protection: Deny by Default/Allow by Exception	-	-	-	-	
SC-7(7)	Boundary Protection: Prevent Split Tunneling for Remote Devices	-	-	-	-	
SC-7(8)	Boundary Protection: Route Traffic to Authenticated Proxy Servers	-	-	-	-	
SC-7(9)	Restrict Threatening Outgoing Communications Traffic	-	-	-	-	
SC-7(10)	Boundary Protection: Prevent Unauthorized Exfiltration	-	-	-	-	
SC-7(11)	Boundary Protection: Restrict Incoming Communications Traffic	-	-	-	-	
SC-7(12)	Boundary Protection: Host Based Protection	-	-	-	-	
SC-7(13)	Boundary Protection: Isolation of Security Tools/Mechanisms/Support Components	-	-	-	-	
SC-7(14)	Boundary Protection: Protects Against Unauthorized Physical Connections	-	-	-	-	
SC-7(17)						-
SC-8	Transmission Confidentiality and Integrity	-	-	-	-	
SC-8(1)	Cryptographic or Alternate Physical Protection	-	-	-	-	
SC-8(2)	PRE / Post Transmission Handling	-	-	-	-	
SC-8(3)	Cryptographic Protection For Message Externals	-	-	-	-	
SC-8(4)	Conceal / Randomize Communications	-	-	-	-	
SC-10	Network Disconnect	-	-	-	-	
SC-15	Collaborative Computing Devices	-	-	-	-	
SC-15(1)	Collaborative Computing Devices: Physical Disconnect	-	-	-	-	
SC-15(3)	Collaborative Computing Devices: Disabling/Removal in Secure Work Areas	-	-	-	-	
SC-17	Public Key Infrastructure Certificates	-	-	-		
SC-19	Voice over Internet Protocol (VoIP)	-	-	-	-	
SC-20	Secure Name/Address Resolution Service (Authoritative Source) & SC-20(1) - Secure Name/Address Resolution Service (Authoritative Source): Child Subspaces	-	-	-	-	

Ctrl Nr	Ctrl Name	SUSA	MUSA	A/V	ISOL	P2P
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver) & SC-21(1) – Secure Name/Address Resolution Service (Recursive or Caching Resolver): Data Origin/Integrity	-	-	-	-	
SC-22	Architecture and Provisioning for Name/Address Resolution Service	-	-	-	-	
SC-23	Session Authenticity	-	-	-	-	
SC-23(1)	Session Authenticity: Invalidate Session Identifiers at Logout	-	-	-	-	
SC-23(3)	Session Authenticators: Unique Session Identifiers with Randomization	-	-	-	-	
SC-23(5)	Allowed Certificate Authorities	-	-	-	-	
SC-42	Sensor Capability And Data	-	-	-		
SC-42(3)	Prohibit Use of Devices	-	-	-		
SI-2(2)	Automated Flaw Remediation Status	-	-	-		
SI-2(3)	Flaw Remediation: Time to Remediate Flaws/Benchmarks for Corrective Action	-	-	-		
SI-3(1)	Malicious Code Protection: Central Management					-
SI-3(2)	Malicious Code: Automatic Updates	-	-	-		-
SI-3(10)	Malicious Code Analysis	G	G	G		
SI-4(1)	Information System Monitoring: System-Wide Intrusion Detection System	-	-	-		-
SI-4(2)	Information System Monitoring: Automated Tools for Real-Time Analysis	-	-	-		-
SI-4(4)	Information System Monitoring: Inbound and Outbound Communications Traffic	-	-	-		-
SI-4(5)	Information System Monitoring: System Generated Alerts	-	-	-		-
SI-4(10)	Visibility of Encrypted Communications	-	-	-		-
SI-4(11)	Information System Monitoring: Analyze Communications Traffic Anomalies	-	-	-	-	
SI-4(12)	Information System Monitoring: Automated Alerts	-	-	-		
SI-4(14)	Information System Monitoring: Wireless Intrusion Detection	-	-	-		

Ctrl Nr	Ctrl Name	SUSA	MUSA	A/V	ISOL	P2P
SI-4(15)	Information System Monitoring: Wireless to Wireline Communications	-	-	-		
SI-4(16)	Information System Monitoring: Correlate Monitoring Information	-	-	-		
SI-4(21)	Probationary Periods	-	-	-		
SI-4(22)	Unauthorized Network Services	-	-	-		
SI-7(14)	Binary or machine executable code	-	-	-		
SI-10	Information Input Validation	-	-	-		

Detailed Overlay Control Specifications

The guidance provided in this section elaborates on the guidance given in NIST SP 800-53 and the JSIG, providing additional insight and guidance on controls and control enhancements identified by this overlay.

AC-3 Access Enforcement

    Supplemental Guidance: Policy for A/V system usage shall restrict users from taking action to save classified information to the A/V system. The A/V system may incidentally store information when classified content is scanned or viruses in classified content are quarantined, but these actions are understood to not represent willful user actions to locally store information.

AC-7 Unsuccessful Logon Attempts

    Supplemental Guidance: The system locks for a minimum of 15 minutes when the maximum unsuccessful logon attempts is reached, but system administrator unlock is not required for a SINGLE user standalone system.

AU-5 Response to Audit Processing Failures

    Supplemental Guidance: For SINGLE; Bullet (a) may be waived, but Bullet (b), "record any audit processing failure in the audit log" shall be implemented.

AU-6 Audit Review, Analysis, and Reporting

    Supplemental Guidance: The frequency of audit review and reporting must be based on the system risk assessment.

IR-4(1) Automated Incident Handling Processes

    Supplemental Guidance: For standalone systems the automated handling processes most likely do not exist on the standalone system itself, but is provided by another system. This control is met by referencing the automated process residing on that other system.

IR-6(1) Automated Reporting

    Supplemental Guidance: For standalone systems the automated reporting processes most likely do not exist on the standalone system itself, but is provided by another system. This control is met by referencing the automated process residing on that other system.

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

Supplemental Guidance: For standalone systems the automated support capability most likely does not exist on the standalone system itself, but is provided by another system. This control is met by referencing the automated support capability residing on that other system.

IR-10 Integrated Information Security Cell

Supplemental Guidance: For standalone systems an integrated security cell most likely exists as a common control provider at a component level organization. This control is met by referencing the organization providing the security cell capability as a common control provider.

SC-4(2) Periods Processing

Supplemental Guidance: Tailor this control in for systems using periods processing. Standalone systems that periods process must provide procedures that meet the requirements of this control and any component level guidance for periods processing.

SI-3(10) Malicious Code Analysis

Supplemental Guidance: For standalone systems malicious code analysis most likely is performed by a common control provider at a component level organization. This control is met by referencing the organization providing the malicious code analysis as a common control provider.

Tailoring Considerations

Additional tailoring of the Standalone Overlay is permitted with the approval of the authorizing official. Tailoring may be needed if additional overlays apply to the information system or to address unique circumstances in the system's environment.

Definitions

There are no new terms defined in this document.

<ORGANIZATION>
<SYSTEM NAME>
<DATE>

Record of Changes:

Version	Date	Sections Modified	Description of Changes
1.0	DD Mm YY	Initial RAR	

System Description
<Insert system name, location, POCs, boundaries, mission, system security categorizations, and type of data processed, classification levels, etc.>

Scope
<Identify assumptions, constraints, timeframe>
The scope of this risk assessment is focused on the system's use of resources and controls to mitigate vulnerabilities exploitable by threat agents (internal and Federal) identified during the RMF control selection process based on the system's categorization.

This initial assessment will be a Tier 3 or "information system level" risk assessment. While not entirely comprehensive of all threats and vulnerabilities to <SYSTEM>, this assessment will include any known risks related to the incomplete or inadequate implementation of the NIST SP 800-53 controls selected for this system. This document will be updated after certification testing to include any vulnerabilities or observations by the independent assessment team. Data collected during this assessment may be used to support higher level risk assessments at the mission/business or organization level.

Purpose
<Why is this being done – initial or subsequent and state circumstances that prompted subsequent assessment>

Example: This initial risk assessment was conducted to document areas where the selection and implementation of RMF controls may have left residual risk. This will provide security control assessors and authorizing officials an upfront risk profile.

Risk Assessment Approach
This initial risk assessment was conducted using the guidelines outlined in the *NIST SP 800-30, Guide for Conducting Risk Assessments*. A *<SELECT QUALITATIVE / QUANTITATIVE / SEMI-QUANTITATIVE>* approach will be utilized for this assessment. Risk will be determined based on a threat event, the likelihood of that threat event occurring, known system vulnerabilities, mitigating factors, and consequences/impact to mission.

The following table is provided as a list of sample threat sources. Use this table to determine relevant threats to the system. Based on the evaluated threats, the risks to the system are listed in Table 6: Risk Assessment Results along with any mitigating factors.

Table 1: Sample Threat Sources (see NIST SP 800-30 for complete list)

TYPE OF THREAT SOURCE	DESCRIPTION
ADVERSARIAL - Individual (outsider, insider, trusted, privileged) - Group (ad-hoc or established) - Organization (competitor, supplier, partner, customer) - Nation state	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications, and the communications and information-handling capabilities provided by those technologies.
ADVERSARIAL - Standard user - Privileged user/Administrator	Erroneous actions taken by individuals in the course of executing everyday responsibilities.

STRUCTURAL
- IT Equipment (storage, processing, comm., display, sensor, controller)
- Environmental conditions
  o Temperature/humidity controls
  o Power supply
- Software
  o Operating system
  o Networking
  o General-purpose application
  o Mission-specific application
	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.

ENVIRONMENTAL - Natural or man-made (fire, flood, earthquake, etc.) - Unusual natural event (e.g., sunspots) - Infrastructure failure/outage (electrical, telecomm.)	Natural disasters and failures of critical infrastructures on which the organization depends, but is outside the control of the organization. Can be characterized in terms of severity and duration.

The following tables from the NIST SP 800-30 were used to assign values to likelihood, impact, and risk:

Table 2: Assessment Scale – Likelihood of Threat Event Initiation (Adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the threat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event

Table 3: Assessment Scale – Likelihood of Threat Event Occurrence (Non-adversarial)

Qualitative	Semi-	Description

Values	Quantitative Values		
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times per year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times per year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times per year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year,** but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

Table 4: Assessment Scale – Impact of Threat Events

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event

			might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Table 5: Assessment Scale – Level of Risk

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	Threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	Threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	Threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	Threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Risk Assessment Results

Threat Event	Vulnerabilities / Predisposing Characteristics	Mitigating Factors	Likelihood (Table 2 or 3)	Impact (Table 4)	Risk (Table 5)
e.g. Hurricane	*Power Outage*	*Backup generators*	*Moderate*	*Low*	*Low*

* Likelihood / Impact / Risk = High, Moderate, Low, or Very Low

APPENDIX F: POA&M TEMPLATE

Plan of Action and Milestones (POA&M)

System Name		Date of this POA&M	
Company/Organization Name		Date of Last Update	
		Date of Original POA&M	

ISSM Information

Name		IS Type	
Phone		UID	
Email			

Item Identifier	Weakness or Deficiency	Security Control	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Changes to Milestones	Weakness/ Deficiency Identified by	Risk Level (Low/Med/High)	Estimated Cost	Status	Comments

Page 248

Authorization	Formal declaration by the AO that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
Authorization to Connect	Formal approval granted by a WAN AO allowing the connection of a node to a WAN.
Authorization to Operate	Approval granted by an AO for an IS to process classified information.
Audit Log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period.
Audit Trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.
Certification	Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements by the ISSM.
Classified Information	Official information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure in the interest of national security and which has been so designated. The term includes National Security Information (NSI), Restricted Data (RD), and Formerly Restricted Data (FRD).
Classified Information Spillage	Security incident that occurs whenever classified data is spilled either onto an unclassified information system or to an information system with a lower level of classification.
Compensating Security Control	A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST Special Publication 800-53 or in CNSS Instruction 1253, that provides equivalent or comparable protection for an information system.
Command Cyber Readiness Inspection	A review of an IS connected to the SIPRNet to evaluate enclave and network security, perform network-based vulnerability scans, and assess compliance with applicable policies.
Company	A generic and comprehensive term which may include sole proprietorships, individuals, partnerships, corporations, societies, associations, and organizations usually established and operating to commonly prosecute a commercial, industrial or other legitimate business, enterprise, or undertaking.
Computer Network Attack	Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
Computer Network Defense	Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.
Controlled Interface (CI)	A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information

	systems (CNSSI 4009).
Confidential	This designation will be applied to information or material the unauthorized disclosure of which could be reasonably expected to damage national security.
Contractor	Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.
Denial	When a Systems Security plan has been accepted and reviewed by an ISSP and is not granted an approval to operate.
Document	Any recorded information, regardless of its physical form or characteristics, including, without limitation, written or printed matter, tapes, charts, maps, paintings, drawing, engravings, sketches, working notes and papers; reproductions of such things by any means or process; and sound, voice, magnetic, or electronic recordings in any form.
Environment	Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an IT system.
Executive Order 12829	The NISP was established by Executive Order 12829, 6 January 1993, "National Industrial Security Program" for the protection of information classified pursuant to Executive Order 12356, April 2, 1982, "National Security Information," or its successor or predecessor orders and the Atomic Energy Act of 1954, as amended.
External System	An information system that is outside of the authorization boundary established by the AO and can be part of interconnected system (contractor-to-government).
Facility	A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For purposes of industrial security, the term does not include Government installations.
Facility (Security) Clearance	An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).
Federal System	Information Systems or components that are outside the authorization boundary of the organization and for which the organization has no direct supervision and authority over the required security controls or the assessment of security control effectiveness.
Field Office Chief	Responsible for managing the DSS Mission across an assigned are of responsibility. IS Reps report to the Field Office Chief.
Formal Access Approval	Formal Access Approval is the documented approval by a data owner to allow access to a particular category of information. It can be linked to any caveated information such as compartmented, NATO, REL TO, Critical Nuclear Weapon Design Information, Communications Security (COMSEC) or Crypto variable information, FRD, etc.
Government Contracting Activity	An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.
Government Furnished Equipment	Property that is acquired directly by the government and then made available to the contractor for use.

|	
Host	The individual who takes ultimate responsibility for preparation and maintenance of accreditation documentation (NSP) for the WAN. Usually the ISSM for one of the nodes, the Host also determines the requirements that must be met before connection to the WAN is permitted.
Information Systems	Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of voice or data, and includes software, firmware and hardware.
Information Systems Security Manager	The contractor employee responsible for the implementation of Automated Information Systems security, and operational compliance with the documented security measures and controls, at the contractor facility.
Information Systems Security Officer	The ISSO(s) is assigned by the ISSM when the facility has multiple authorized ISs, is in a multiple facility organization in which the ISSM has oversight responsibility for multiple facilities, or when the technical complexity of the facility's IS program warrants the appointment. The name and phone number of the ISSO(s) must be identified in the SSP(s). During an IS certification visit the IS Rep or ISSP will determine what duties and responsibilities have been delegated to the ISSO and verify the ISSO understands them. During a Security Review, the IS Rep or ISSP will review those duties and responsibilities and verify the ISSO is carrying them out.
Interconnection Security Agreement	Contract between telecommunication organizations for interconnecting their networks and exchanging telecommunication traffic.
Interim Approval to Connect	Temporary approval granted by a WAN AO allowing the connection of a node to WAN.
Interconnected System	An interconnected network consists of two or more separately authorized systems connected together. Interconnected networks may be contractor-to-contractor or government-to-contractor connections, or a combination of both.
Interim Approval to Operate	Temporary approval granted by an AO for an IS to process classified information.
Internet Protocol	Connectionless protocol used in packet-switched layer networks, such as Ethernet.
Local Area Network	Computer network within a small geographical area such as a home, school, computer laboratory, office building or group of buildings.
Master Systems Security Plan	The term "Master" indicates the authorization to add IS to an approved plan by an ISSM using Type Authorization.
Multiple User Stand-Alone	Systems that have one user at a time, but have a total of more than one user with no sanitization between users, as Multiuser systems.
National Institute of Standards and Technology	Organization that promulgates national level standards, including those designed to protect IS.
Network	An IS term meaning a network composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include ISs, packet

	switches, telecommunications controllers, key distribution centers, and technical control devices.
Network Security Plan	Document(s) submitted by the WAN owner to the WAN AO that describes the security features and requirements of the WAN.
NISP Authorization Office	Delegated the responsibility for the DSS mission for cleared contractor IS certification and accreditation oversight.
Node	Any device or collection of devices authorized under a single Systems Security plan connected to a WAN.
Physical Security	The measures used to provide physical protection of resources against deliberate and accidental threats.
Plan of Action and Milestones	Facilitates an agreement between the contractor and DSS identifying items from the baseline configuration requirements cannot be met and the reasons. The POA&M documents deficiencies that can be corrected and defines a timeline for resolving the issues.
Protected Distribution System	Secure conduit for protecting classified lines, transmitting data outside of a controlled area.
Radio Frequency ID	Technologies that use wireless communication between an object (also known as a tag) and an interrogating device (also known as a reader), for the purposes of automatically tracking and identifying of such objects.
Re-Authorization	An action taken by DSS when security relevant changes are made to an approved (M)SSP. An action taken by DSS 3 years from the date of the ATO for a (M)SSP.
Regional Director	Responsible for all aspects of operations within the region.
Risk	A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.
Risk Acknowledgement Letter	Letter from the GCA acknowledging the level of risk when an information system cannot be configured to meet requirements of the NISPOM based on customer defined requirements.
Risk Assessment	Process of analyzing threats to, and vulnerabilities of, an IT system, and the potential impact that the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and effective measures.
Risk Management	Process concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected.
SECRET	The designation that will be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
Secure Terminal Equipment	Piece of equipment utilized to enable encrypted/secure voice and/or data communication.
Security Cognizance	The Government office assigned the responsibility for acting for CSAs in the discharge of industrial security responsibilities described in the NISPOM.
Security-Relevant Change	A security-relevant change to a system is any change affecting the availability, integrity, authentication, confidentiality, or non-repudiation of an IS or its environment. Examples would include changes to the

	Identification and Authentication, Auditing, Malicious Code Detection, Sanitization, Operating System, Firewall, Router Tables and Intrusion Detection Systems of a system, or any changes to its location or operating environment.
Security Requirement	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.
Single User Stand-Alone	Systems assigned to single user and are without network connectivity.
Systems Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
TOP SECRET	The designation that will be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
Telecommunications Electronics Material Protected from Emanating Spurious Transmissions	The protection of sensitive information being compromised from electronic equipment producing emanations.
User	Person or process authorized to access an IT system.
User Code	Software that allows a user to modify data or functions of an IS. Determining if an IS has user code may be a matter of degree, but as an example, if an IS only has a button that performs a single function when pressed, the system is considered to have no user code on it. If the user can input classified information and save it to the IS then the IS certainly has user code.
Video Teleconference	Technology that facilitates the communication and interaction of two or more users through a combination of high-quality audio and video over Internet Protocol networks.
Voice Over Internet Protocol	Technology used for delivering different kinds of data from a source to a destination using IP (Internet Protocol).
Wide Area Network	Network that exists over a large-scale geographical area.

APPENDIX H: DSS RMF PROCESS

DSS Risk Management Framework (RMF) Process   APRIL 2016
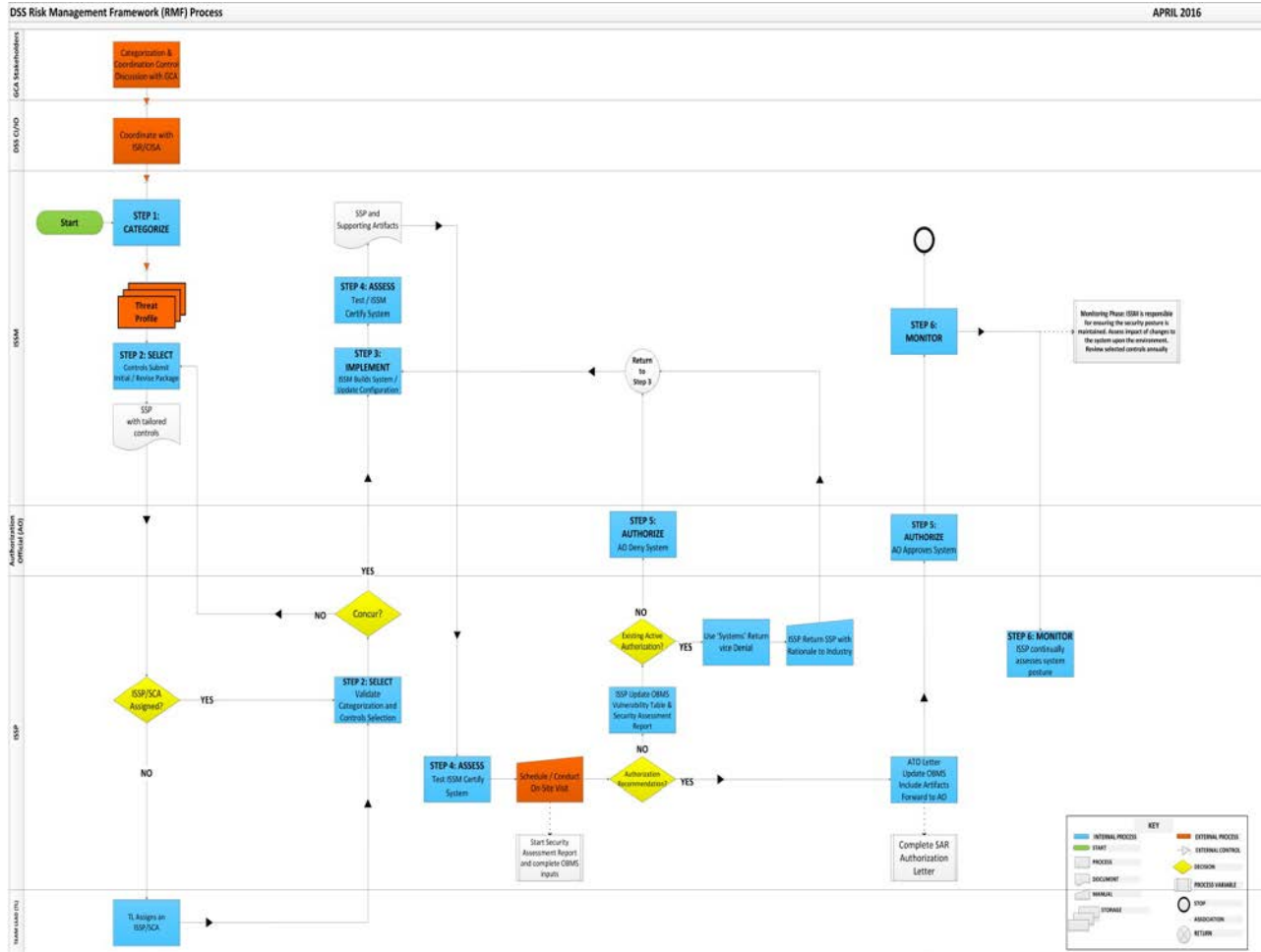
APPENDIX I: ISSM CERTIFICATION STATEMENT

To: Defense Security Service
      27130 Telegraph Road
      Quantico, VA 22134

   Subject: RMF IS Security Package Submission and Certification Statement

   This letter serves as notification that the systems identified in the attached SSP (or in the NAO Unique Identifier below) have been certified.

Facility Name:	CAGE Code:
Address:	
ISSM/Phone:	
NAO Unique Identifier:	

By submitting this security package I am providing formal certification that the requirements and implementation procedures listed within the attached System Security Plan (SSP) Procedures is in accordance with National Industrial Security Process Manual (NISPOM), National Institute of Standards and Technology (NIST 800-53) and the DSS Assessment and Authorization Manual. I certify that all security controls and protection measures as described in the attached System Security Plan and attachments have been implemented and are operational on the above named systems. I understand that failure to comply with the above conditions could result in the withdrawal of existing authorization. Any items that do not meet all NISPOM and DAAPM requirements will be addressed in a Plan of Action and Milestone (POA&M).

By signing below I certify that the information provided in the attached security package is true and correct. I also understand that my submission of this letter and the attached security package constitutes a statement on a matter within the jurisdiction of the Executive Branch of the United States. I understand that the United States Criminal Code (Title 18, section 1001) provides that making willful false official statements or concealing a material fact in this information system security package is a felony which may be punished by fine or imprisonment or both.

Thank You,

ISSM Signature   Date

DSS Authorized Warning Banner
Use of this U.S. Government (USG)-interest computer system constitutes consent for authorized monitoring at all times.

This is a USG-interest computer system. This system and related equipment are intended for the communication, transmission, processing, and storage of official USG or other authorized information only. This USGUSG-interest computer system is subject to monitoring at all times. to ensure proper functioning of equipment and systems including security systems and devices, and to prevent, detect, and deter violations of statutes and security regulations and other unauthorized use of the system.

Communications using, or data stored on, this system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any authorized purpose.

If monitoring of this USG-interest computer system reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring of this USG-interest computer systems reveals violations of security regulations or other unauthorized use that information and other related information, including identification information about the user, may be used appropriate administrative or disciplinary action.

Use of this USG interest computer system constitutes consent to authorized monitoring at all times. |

DoD SIPRNet Warning Banner
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. |

Table of DSS Authorized File Type/Formats

Format Type	Explanation	Common File Extension(s)
ASCII	ASCII formatted information is essentially raw text just like the words you are reading now. Many applications have the ability to export data in ASCII or text format. Program source code, batch files, macros and scripts are straight text and stored as ASCII files. ASCII files may be read with any standard text editor.	.txt .dat .c .for .fil .asc .bat *(Note: This is not an all-inclusive list. If a file cannot be read with a standard text editor, try changing the extension to .txt. If the file still cannot be read with a text editor, it is most likely not an ASCII file.)*
Hypertext Markup Language	The document format used on the World Wide Web. Web pages are built with HTML tags (codes) embedded in the text. HTML defines the page layout, fonts and graphic elements as well as the hypertext links to other documents on the Web.	.html .htm
JPEG	Joint Photographic Experts Group (pronounced jay-peg) An ISO/ITU standard for compressing still images that is very popular due to its high compression capability.	.jpg
BMP	A Windows and OS/2 bitmapped graphics file format. It is the Windows native bitmap format. Every Windows application has access to the BMP software routines in Windows that support it.	.bmp
Graphics Interchange Format	A popular bitmapped graphics file format developed by CompuServe.	.gif

Note: Executable programs may not be transferred. The source code (ASCII text) may be reviewed/transferred to a lower level IS then re-compiled into executable code.

(Government letterhead)

[GCA/Data Owner Name]
[Address]

SUBJECT: Acceptance of Risk to Classified Information

TO: [Contractor]

Reference National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, Chapter 8, February 28, 2006 (http://www.dss.mil).

Paragraphs 8-302a, 8-305, 8-306b, 8-309, 8-310a,b 8-401, 8-610a(1)c; permit the transfer of unclassified or lower classified information from an Information System (IS) accredited by the Defense Security Service (DSS). DSS has identified certain file formats and procedures that are authorized for this transfer. However, the particular file format/procedure is not robust enough for the type or amount of information that we require.

Working in combination with a DSS Information Systems Security Professional (ISSP), an alternative to the DSS procedure for [file format(s)] has been developed. It is understood that this alternative procedure, though considered safe, increases the risk of compromise to classified information. In order to use this alternative procedure, DSS requires that the additional risk be identified to, and accepted by, the GCA or data owner.

The alternative procedure is attached for your review. If you agree with the alternative procedure and paragraph 5, please sign and return to the above address. If you have any questions, I may be reached at the number below.

It is understood that there is an inherent risk associated with the transferring of unclassified or lower classified information from a DSS accredited IS to unclassified or lower classified media. The undersigned concurs that a trusted download is necessary for [contractor name] to adequately perform work on our behalf and we accept the Alternate Procedures falls well within the governments standards for acceptable risk.

_____
Signature
Customer/sponsor or data owner

_____
Printed Name Phone #

Date	Person	File Type	File Description

For the Movement of Classified Information Systems (IS)

Facility
Address
City, State Zip Code

Date of Mobility Plan
Revision Number

A. Introduction
This plan outlines the procedures for the transporting of classified IS equipment between [Facility], and various sites as listed in the Mobile Processing Plan attached to the IS Profile.

B. Description of Equipment
Equipment consists of computers, components and test equipment to be used in support of field tests, flight test, customer reviews and meetings. See IS Profile for list of equipment.

C. Identification of Participating Government and Contractor Representatives
- [Facility]
- Name of ISSM
- Address
- Contact information
- Local Defense Security Service Representative
- Name of IS Representative
- Address
- Contact information

D. Shipping and Transportation
Movement of the equipment will originate from [Facility]. Equipment will be transported to various sites listed in the Mobile Processing Procedures attached to the IS Profile. The ISSM will notify the DSS Representative prior to shipping the system to/from any off-site location. All equipment will be shipped either as classified at system approval level or downgraded to an unclassified state, security seals affixed. All remaining classified components will be properly shipped or hand carried.

E. Notification of Transportation
The ISSM will be notified of the upcoming shipment as early as possible.
The following information must be provided:
- Program name
- Classification
- Will the shipment contain hazardous material? If so, provide MSDS sheet or IHC letter from customer
- Size and weight of equipment
- Who owns the equipment, is it GFE?

F. Hand Carry (Courier)

You are reminded that hand carry (courier) is only done in emergency situations. When couriers are to be used, the program must justify why a hand carry must occur rather than utilizing approved classified mailing or shipping capabilities. This must be authorized by the Security Manager. Each courier must be identified by name, title, payroll number, as well as the name of the program being supported. Flight itinerary and vehicle rental information must be furnished. Couriers must be cleared at the appropriate level and be thoroughly briefed on their security responsibilities. Each courier will be issued a "Courier Authorization" and will be provided emergency telephone numbers.

G. Responsibilities of Receiving Facility

- The recipient organization must notify the dispatching organization and [Facility] Security of any security relevant problems that occur.
- The recipient organization must notify the dispatching organization and [Facility] Security of any discrepancies in the documentation or equipment.

CONTRACTOR LETTERHEAD
(To be used when releasing IS to government activity or test site.)

(DATE)

FROM: (ISSM)
TO: (Name of government site ISSO and address)

SUBJECT: Relocation of DSS Accredited Information System (name or number of IS) from (company name) to (user agency site or test-site).

On (accreditation date) the Defense Security Service (DSS) accredited under the National Industrial Security Program Operating Manual (NISPOM) information system (IS) (name or number of IS) located at (company name) to process classified information at the (level of classified information) level. A copy of the accreditation letter is attached for your review.

(Company name) has a requirement in conjunction with (contract number) with (name of GCA) to relocate the above to (name of government site or test site) in order to process classified information for (purpose). During the period when this will be resident at (name of government site, test site, or installation, etc.) your activity must assume cognizance for the security of the system. Any movement of an accredited IS outside of the DSS-approved area changes the original intent of DSS' accreditation. As you are aware, different risks and vulnerabilities are associated with moving an IS, to include, for example, different threats to the IS or classified information, different physical security factors and different user need-to-know concerns.

Prior to the above system being relocated to your site, an authorized official of (name of site) must sign this letter and return it to the address provided. Your authorized official's signature will represent your organization's concurrence to accept security cognizance for the above-specified IS while it will be located at your site and under your jurisdiction. (Name of contractor) anticipates the IS (or closed area) will be removed from (name of site), and consequently your jurisdiction, by (provide approximate time of removal and location to which the system will be subsequently relocated).

If you have questions or would like to discuss this, please contact (company POC) at (telephone number) or by e-mail at (e-mail).

Sincerely,

(ISSM's Name)
(Title/Company)
Attachments: DSS Accreditation Letter
Dated (Date)
Copy to: (Cognizant DSS ISR)
CONCURRENCE:

_____
(Name/Title of Authorized Official)

Printed Name:	Job Function or Title:

Manager Request

I request the above named individual be authorized to perform Trusted Downloads. I understand this access requires training to perform Trusted Downloads, a process for generating unclassified or lower classified media from a classified system. I understand this process involves both knowledge of classification issues and attention to detail in reviewing information and following the process for performing a download. I also understand that transferring information from a classified environment to an unclassified environment increases the risk of compromising classified information and will instruct authorized employees under my supervision to perform these actions only when absolutely necessary.

Printed Name:

Signature:	Date:

Acceptance of Responsibility

I have attended a Trusted Download training class and understand both the risks associated with performing a Trusted Download and the mechanisms associated with the Trusted Download process. I understand that all media generated from a classified system must be labeled and handled at the highest level of data on the system unless a Trusted Download Procedure is performed. I understand it is my responsibility to perform this process as outlined in the Trusted Download Procedure.

Signature:	Date:

ISSM or ISSO Authorization

I certify that the individual identified above has been briefed in the vulnerabilities associated with transferring unclassified or lower classified information from an accredited Information System (i.e., trusted download). Additionally, he/she has demonstrated extensive knowledge of all appropriate security classification guide(s) and authorized procedures associated with the information downloaded.

Authorized File Formats: ASCII/Text, HTM/HTML, JPEG, BMP, GIF
Specify:

Printed Name:

Signature:	Date: