DEPARTMENT OF DEFENSE (DOD)

JOINT SPECIAL ACCESS PROGRAM (SAP) IMPLEMENTATION GUIDE (JSIG)

11 April 2016

NOTE:
This version of the JSIG is based on NIST SP 800-53, Rev 4 and CNSSI 1253, March 2014.

PREFACE

The Risk Management Framework (RMF) is a framework designed to be tailored to meet organizational needs while providing adequate risk management of data and information systems. Transformation to the RMF is a daunting task and we appreciate all the effort to date within the Department and Industry. We applaud all the hard work of the Joint SAP Cybersecurity Working Group (JSCS WG) and the spectacular leadership of the individuals who created this joint “coalition of the willing.”

Special Access Programs represent some of the Department’s most sensitive information and must be protected accordingly. We can no longer rely on physical isolation as a primary risk mitigation strategy. Threats and risks often outpace our ability to implant robust, multi-disciplinary countermeasures. Cost and timelines to develop threats to our data almost always pale to the cost and time to implement countermeasures. Given the rapid increase in cybersecurity threats and prioritization from the SECDEF, the senior cybersecurity professionals responsible for authorizing information systems to process SAP have identified three security controls which offer mitigations so significant they can no longer be tailored. Beginning in this revision of the JSIG, we are introducing controls that are not tailorable. Historically, the ability to tailor controls has been delegated to the field but senior leadership is no longer willing to accept the risk of high volume data loss. Recognizing there may be extreme situations in which it is not feasible to implement these controls in their entirety, the authority to tailor or modify these controls is delegated to the component SAP senior authorizing official. This waiver authority cannot be further delegated. The establishment of a senior authorizing official for each DoD component will elevate the status of cybersecurity functions so they more effectively influence department-wide strategy, policy, and investments.

Summary of Changes:

- Establishment of Component SAP Senior Authorizing Officials
  - Each DoD component responsible for authorizing SAP information systems, shall assign in writing a SAP Senior Authorizing Official for the component. This SAP Senior Authorizing Official shall be the waiver authority for “non-tailorable controls.” This authority cannot be delegated. Waivers to these controls will be submitted to the DoD SAPCO and DoD SAP CIO within 30 days of approval.
- Establishment of non-tailorable controls
  - See AC-6(1), Least Privilege | Authorize Access to Security Functions
    - System endpoint protection shall not be tailored out.
  - See SA-22,Unsupported System Components
    - Added to the baseline and required to be implemented on all SAP systems.
  - See SC-28, Protection of Information at Rest
    - Encryption of data at rest shall be implemented for all SAP systems.
- The entirety of this document is effective immediately.

Policy

The policy of the U.S. Government is that all classified information be appropriately safeguarded to assure the confidentiality, integrity, and availability of that information. This document provides standardized security policies and procedures for use in the management of all networks, systems, and components under the purview of the Department of Defense (DoD) Special Access Program Central Office (SAPCO) and DoD Service/Agency SAPCOs. This guidance applies to the DoD SAP Community and all networks, information systems, weapon systems, and applications for which the cognizant SAP Authorizing Official (AO) has management or oversight responsibility, regardless of the physical location.

Responsibilities

The Joint SAP Cybersecurity Working Group (JSCS WG) is chartered to provide DoD SAP cybersecurity implementation guidance. The JSCS WG provides organizations within the DoD SAP Community a forum to address all aspects of cybersecurity. JSCS WG functions and activities related to RMF include:

- Promote DoD SAP Community coordination in methodologies for assessing and authorizing SAP information systems and related areas (e.g., documentation, tools, assessment methods, processes) to provide for consistency in methodologies, approaches, templates, and organization-defined values across the DoD SAP Community
- Develop, maintain, and periodically update the policies and procedures related to RMF to include, as needed, JSIG, security control overlays, RMF training, templates, and other supporting documentation
- Promote, review, and update training and awareness objectives, material, and availability for all service, agency, and industry partners on cybersecurity, emphasizing insider threat, community best practices, and RMF

Additional information on roles and responsibilities related to the Risk Management Framework can be found in Section 1.5.

Effective Date

This document is effective immediately and organizations should begin tracking the changes from the Revision 3 to Revision 4 security controls (new, modified and deleted) in an information system POA&M, with a focus on the three non-tailorable controls identified above. Components may also provide additional transition guidance.

This document must be reissued, cancelled, or certified current within 5 years of its publication to be considered current.

David B. Bèen
Brigadier General, USAF
Director, Special Access Program Central Office

Kenneth R. Bowen
Chief Information Officer for
DoD Special Access Programs

Table of Contents

Table of Figures

Table of Tables

1 INTRODUCTION AND ROLES

1.1 INTRODUCTION

The DoDM 5205.07, Volume 1, *Special Access Program (SAP) Security Manual: General Procedures*, provides policy, guidance, and standards for the authorization of information systems and application of RMF within a DOD SAP. OSD Memorandum for Special Access Program Senior Working Group Members, Subject: *Transition to the Risk Management Framework*, dated December 18, 2013, provides guidance to assist the DoD SAP Community in meeting congressionally mandated implementation guidelines in the transition from Joint Air Force – Army – Navy (JAFAN) 6/3 Manual, *Protecting Special Access Program Information within Information Systems* to RMF.

The documents having a key role in the assessment and authorization of DoD SAP information systems include:

- DoDD 5205.07, *Special Access Program (SAP) Policy*
- DoDM 5205.07 SAP Security Manual:
    - Volume 1 (V1) *General Procedures*
        - Reference Enclosure 6, *Cybersecurity*
    - Volume 2 (V2) *Personnel Security*
    - Volume 3 (V3) *Physical Security*
    - Volume 4 (V4) *Marking*
- NIST Special Publications (SP) Joint Task Force (JTF) Initiative documents:
    - NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
    - NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
    - NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
    - NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
    - NIST SP 800-30, *Guide for Conducting Risk Assessments*
- CNSSI 1253, *Security Categorization and Control Selection for National Security Systems, March 27, 2014*
- *Joint SAP Implementation Guide* (JSIG)
- *DoD 8570.01-M Information Assurance Workforce Improvement Program* or its replacement based on DoDD 8140.01, *Cyberspace Workforce Management*

RMF provides organizations with a disciplined, structured, flexible, and repeatable process for managing risk related to the operation and use of information systems (IS). The CNSS describes information system security categorization and security controls selection for National Security Systems (NSS). The DoD is ensuring that its policies and procedures comply with the CNSS standards (e.g., CNSSI 1253) allowing the DoD SAP Community to more efficiently support reciprocity.

DoD Instruction (DoDI) 5205.11, *Management, Administration, and Oversight of DoD Special Access Programs (SAPs)* requires that elements of the DoD SAP Community establish, publish, issue, and promulgate information technology (IT) risk management standards for the DoD SAP Community. The RMF and applicable standards, policies, and guidelines published by NIST and CNSS support this instruction.

1.2 PURPOSE AND APPLICABILITY

The purpose of this document is to provide policy and guidance on the implementation of the RMF. This document, the JSIG, serves as a technical supplement to NIST SP 800-53 and CNSSI 1253, and is used in concert with the applicable volume of DoDM 5205.07 in the application of the RMF. JSIG provides standardized cybersecurity/information assurance-related policy, procedures, and implementation guidance for use in the management of all networks, systems, and system components at all classification levels under the purview of the cognizant SAP Authorizing Official (AO). These policies and procedures adhere to applicable laws, Executive Orders (EO), directives, policies, regulations, standards, and guidance.

The security policy and procedures contained in this document are intended for use by all personnel with a responsibility for protecting the confidentiality, integrity, and availability of DoD SAP information, information systems, and networks. This document applies to the DoD SAP Community and all networks, information systems, and applications for which the cognizant SAPCO has management or oversight responsibility regardless of the physical location. This includes Service elements, contractor sites, and DoD organizations that connect to a SAP-managed network. This document supersedes all previous dated versions of the JSIG.

As defined in CNSSI 4009, *Committee on National Security Systems (CNSS) Glossary*, an information system is defined as, "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." This includes weapons systems, test equipment, multifunction devices (e.g., copier/fax/scanner), et al. Information system components are either purchased commercially off-the-shelf (COTS) or are custom-developed and can be deployed in land-based, sea-based, airborne, space-based, and/or tactical IS.

All SAP IS are categorized as NSS as established in the Federal Information Security Management Act (FISMA), Title II, Public Law 107-347, December 17, 2002 (Section 3542, Paragraph (2)(A)(ii)), and further described in NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

1.3 RECIPROCITY

Reciprocity is defined as a "Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information." [CNSSI 4009]

This agreement, however, 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 (e.g., system security plan (SSP), test plans, test procedures, test reports, exceptions) and determine if there are any deltas in the evidence, (e.g., baseline/overlay controls that were tailored, a test item that was omitted), 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.

1.4 CHANGES IN TERMINOLOGY

Table 1-1 provides a mapping between terminology previously associated with the process formerly referred to as certification and accreditation and the new terminology adopted under the RMF.

Old Term	New Term
Certification and Accreditation (C&A) Process	Risk Management Framework (RMF)
Certification	Assessment
Accreditation	Authorization
Requirements	Controls
Protection Level (PL) - PL1/PL2 - PL3/PL4/PL5	Accessibility - Baseline - Baseline + appropriate overlay, e.g., Cross Domain Solution (CDS) Overlay
Level of Concern	Impact Level
Security Requirements Traceability Matrix (SRTM)	Security Controls Traceability Matrix (SCTM)
System Security Authorization Agreement (SSAA) / System Security Plan (SSP)	SSP
Certification Test and Evaluation (CT&E) / Security Test and Evaluation (ST&E) Report	Security Assessment Report (SAR)
Designated Accrediting Authority (DAA)	Authorizing Official (AO)
Chief Information Assurance Officer (CIAO)	Chief Information Security Officer (CISO)
Certifier / Certification Authority / Service Certifying Organization (SCO) / Information System Security Professional (ISSP)	Security Control Assessor (SCA)
DAA Representative	Varies depending on service/agency
No equivalent	Delegated Authorizing Official (DAO)
No equivalent	Risk Executive (Function) (REF)
No equivalent	Common Control Provider (CCP)
No equivalent	Overlay (e.g., Accessibility, CDS, Standalone)
Information Assurance Manager (IAM)	Information System Security Manager (ISSM)
Information Assurance Officer (IAO)	Information System Security Officer (ISSO)
Program Manager (PM)	Information System Owner (ISO)*
Information System Security Engineer (ISSE)	ISSE
Master SSP (MSSP)	Information Assurance Standard Operating Procedures (IA SOP)
Guest System	External Information System
* The ISO is the official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. PM and ISO terms may be used interchangeably.	

Table 1-1: Changes in Terminology

1.5 ROLES AND RESPONSIBILITIES

The roles and responsibilities of the personnel involved with the RMF are summarized in the paragraphs below. Roles and responsibilities are detailed in NIST SP 800-37, Appendix D. Also reference DoDM 5205.07-V1.

1.5.1 Agency/Component Head

Each DoD SAP Component Head bears ultimate responsibility for mission accomplishment and execution of business functions, and hence for adequately mitigating risks to the element, its individuals, and the Nation. The Component Head establishes priorities to ensure collaboration and information-sharing sufficient to ensure both element and DoD SAP Community-wide mission accomplishment. As stated in DoDD 5205.07 Enclosure 5, DoD Component Heads appoint a DAA [AO] for all DoD IS and PIT [Platform IT] systems under their purview and ensure all DoD IS and PIT systems are authorized. DoD SAP systems shall be authorized in accordance with DoDM 5205.07-V1 and the JSIG. Each component shall also establish in writing, the component's SAP senior authorizing official. This individual shall serve as the component lead at DoD level SAP cybersecurity strategy, policy, and, as appropriate, investment forums. The SAP senior authorizing official is the only authorized waiver authority for non-tailorable controls.

Reference DoDM 5205.07-V1, Enclosure 2, for responsibilities of the DoD Component Heads and OSD Principal Staff Assistants (PSA) with cognizant authority (CA) and oversight authority (OA) over SAPs.

1.5.2 Risk Executive (Function)

The Risk Executive (function) (REF) is an individual or group within an organization that helps to ensure that:

- Risk-related considerations for individual IS, to include authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions; and
- Managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success.

The REF coordinates with the senior leadership and stakeholders of an organization to:

a. Provide a comprehensive, organization-wide, holistic approach for addressing risk—an approach that provides a greater understanding of the integrated operations of the organization;

b. Develop a risk management strategy for the organization providing a strategic view of information security-related risks with regard to the organization as a whole;

c. Facilitate the sharing of risk-related information among authorizing officials and other senior leaders within the organization;

d. Provide oversight for all risk management-related activities across the organization (e.g., security categorizations) to help ensure consistent and effective risk acceptance decisions;

e. Ensure that authorization decisions consider all factors necessary for mission and business success;

f. Provide an organization-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, other organizations, and national security;

g. Promote cooperation and collaboration among AOs and stakeholders to include authorization actions requiring shared responsibility, e.g., for reciprocity;

h. Ensure that the shared responsibility for supporting organizational mission/business functions using external providers of information and services receives the needed visibility and is elevated to the appropriate decision-making authorities; and
i. Identify the organizational risk posture based on the aggregated risk to information from the operation and use of the information systems for which the organization is responsible.

The REF serves as an adjunct advisor providing support to the AO/DAO. The REF has no authorization authority. The REF must be comprised of U.S. citizens that are government employees.

1.5.3 Chief Information Officer (CIO)

The CIO is an organizational official responsible for:

- Designating a Chief Information Security Officer (CISO);
- Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements;
- Overseeing personnel with significant responsibilities for information security and ensuring that personnel are adequately trained;
- Assisting senior organizational officials concerning their security responsibilities; and
- In coordination with other senior officials, reporting annually to the head of the agency on the overall effectiveness of the organization's information security program, including progress of remedial actions.

The CIO must be a U.S. citizen and a government employee. The CIO, with the support of the REF and the CISO, works closely with the AO and their designated representatives to help ensure that:

a. An organization-wide information security program is effectively implemented resulting in adequate security for all organizational IS and environments of operation for those systems;
b. Information security considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, and acquisition/system development life cycles;
c. Information systems are covered by approved security plans and are authorized to operate;
d. Information security-related activities required across the organization are accomplished in an efficient, cost-effective, and timely manner; and
e. There is centralized reporting of appropriate information security-related activities.

1.5.4 Chief Information Security Officer (CISO)

The CISO, also known as a Senior Information Security Officer (SISO), is responsible for carrying out the CIO security responsibilities under FISMA. The CISO serves as the primary liaison for the CIO to the organization's AOs, Information System Owners (ISO), Common Control Providers (CCP), and Information System Security Managers/Officers (ISSM/ISSO). The CISO must be a U.S. citizen and a government employee.

The CISO shall:

- Possess professional qualifications, including training and experience, required to administer the information security program functions;
- Maintain information security duties as a primary responsibility; and
- Head an office with the mission and resources to assist the organization in achieving more secure information and IS, in accordance with the guidance provided by their respective CA for FISMA compliance. All FISMA activities shall be maintained within channels and reported to the CA SAPCO.

The CISO may also be appointed with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. [PM-2]

1.5.5 Authorizing Official (AO)

The AO is a 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. The AO must be a U.S. citizen and a government employee. AOs typically have budgetary oversight for an IS or are responsible for the mission and/or business operations supported by the system. Through the security authorization process, AOs are accountable for the security risks associated with information system operations. Accordingly, AOs are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks.

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 security requirements;
b. Evaluate threats and vulnerabilities to information systems to ascertain the need for additional safeguards;
c. Issue and maintain written security authorization statements;
d. Ensure records are maintained for all IS authorizations under his/her purview;
e. Ensure a security education, training, and awareness program is in place;
f. Ensure information system security is an element of the life-cycle process;
g. Ensure all DAOs and security control assessors (SCAs) are trained to properly perform their duties;
h. Ensure all assessments are coordinated with the CA Program Security Officer (PSO);
i. Ensure organizations plan, budget, allocate, and spend adequate resources in support of IS security;
j. Approve security plans, memorandums of agreement or understanding, and plans of action and milestones and determine whether significant changes in the information systems or environments of operation require reauthorization;
k. Deny authorization to operate an information system or if the system is operational, halt operations, if unacceptable risks exist;
l. Coordinate their activities with the REF, CIO, CISO, CCP, ISO, ISSM/ISSO, SCA, and other interested parties during the security authorization process; and,
m. Authority to specify, notwithstanding the requirements stated in this JSIG, a greater impact level or amount of protection for any given system in any given environment.

With the increasing complexity of missions/business processes, partnership arrangements, and the use of external/shared services, it is possible that a particular information system may involve multiple authorizing officials. If so, agreements are established among the authorizing officials and documented in the security plan.

An AO may appoint one or more Delegated Authorizing Official (DAO) to expedite authorizations of designated systems, and provide mission support. Authorizing officials are responsible for ensuring that all activities and functions associated with security authorization that are delegated to authorizing official designated representatives are carried out.

1.5.6 Delegated Authorizing Official (DAO)

The DAO is an organizational official appointed in writing and authorized to act on behalf of an AO in carrying out and coordinating the required activities associated with security authorization including, when explicitly delegated, the authority to authorize a system to operate. A DAO has inherent U.S. Government authority and, as such, must be a government employee. Like an AO, a DAO shall have a broad and strategic understanding of the DoD SAP Community. A DAO shall use this knowledge to assign appropriate weight to the often competing equities of mission and security requirements, budget consequences, operational performance efficiencies, schedule requirements, counterintelligence concerns, civil liberty and privacy protection, and other relevant policy requirements. Then, in light of these factors, the DAO shall determine the level of risk deemed acceptable when authorizing systems. DAOs can be empowered by AOs to make certain decisions with regard to the planning and resourcing of the security authorization process, approval of the SSP, approval and monitoring the implementation of a Plan of Action and Milestones (POA&M), and the assessment and/or determination of risk. The delegation letter must outline specific authorities including impact levels, i.e., low, moderate, or high for confidentiality, integrity, and availability.

1.5.7 Security Control Assessor (SCA)

A SCA is an individual appointed in writing by the AO to act on his or her behalf to conduct a security assessment. The SCA is responsible for 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). SCAs also provide 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.

Prior to initiating the security control assessment, the SCA reviews the SSP to ensure the plan provides a set of security controls for the IS that meet the stated security requirements. Within the DoD SAP Community an ISSM or other AO designee may be delegated in writing to perform security control assessments for specific information systems on the SCA's behalf. These designees must send their assessment results to the SCA for further action.

Responsibilities of the SCA, under the direction of the AO, include, but are not limited to:

a. Advise the ISO and PSO concerning the impact levels for confidentiality, integrity, and availability for the information on a system;
b. Evaluate threats and vulnerabilities to information systems to ascertain the need for additional safeguards;
c. Review and approve the information system Security Assessment Plan, which is comprised of the SSP, the SCTM, and the Security Control Assessment Procedures;
d. Ensure security assessments are completed for each IS;
e. At the conclusion of each security assessment activity, prepare and submit the final Security Assessment Report (SAR) containing the results and findings from the assessment and a recommended authorization decision to the AO;
f. Ensure system POA&M reflects identified weaknesses and suspense dates for each IS based on findings and recommendations from the SAR;
g. Evaluate security assessment documentation and provide written recommendations for security authorization to the AO;
h. Submit the security authorization package to the AO; and

i. Assess proposed changes to information systems, their environment of operation, and mission needs that could affect system authorization.

1.5.8 Common Control Provider (CCP)

A CCP is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common security controls (i.e., security controls inherited by information systems).

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

a. Document the organization-identified common controls in a SSP;
b. Ensure that required assessments of common controls are carried out by qualified assessors;
c. Document assessment findings in a SAR; and
d. Produce and maintain a POA&M for all common security controls having weaknesses or deficiencies; and,
e. Ensure SSPs, SARs, and POA&Ms for common controls are made available to ISOs inheriting those controls.

1.5.9 Program Security Officer (PSO)

Reference DoDM 5205.07, *SAP Security Manual*, all volumes.

1.5.10 Information Owner/Steward

An information owner 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 information owner/steward must be a U.S. citizen and a government employee. Each respective CA SAPCO shall also serve as the information owner/steward. In information-sharing environments, the information owner/steward is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with or provided to other organizations. The owner/steward of the information processed, stored, or transmitted by an information system may or may not be the same as the ISO. A single information system may contain information from multiple information owners/stewards. Information owners/stewards provide input to ISOs regarding:

- Sensitivity of information under the information owner/steward's purview;
- Confidentiality, integrity, and availability impact levels associated with the information owner/steward's data;
- Unique requirements for managing the information owner/steward's data (e.g., incident response, information contamination to other systems/media, unique audit requirements); and,
- Whether foreign nationals may access the information owner/steward's data.

1.5.11 Mission/Business Owner (MBO)

The MBO has operational responsibility for the mission or business process supported by the mission/business segment or the information system and is the key stakeholder for system lifecycle decisions (e.g., agency/component head, chief executive officer, chief financial officer). The MBO ensures that information security requirements are integrated into the system development life cycle process. The MBO must be a U.S. citizen and a government employee.

1.5.12 Information System Owner (ISO)

An ISO is an organizational official, (i.e., government PM or contractor PM (for contractor owned systems)) responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The ISO is responsible for addressing the operational interests of the user community (i.e., users who require access to the information system 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 information systems under their purview;

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

c. Ensure development and maintenance of the documentation required for authorization to operate (e.g., SSP, SAR, POA&M) and that the system is deployed and operated in accordance with the agreed-upon security controls;

d. Determine, in coordination with the information owner/steward, the individuals eligible for access to the system and the types of privileges or access rights required;

e. If required to meet DoDI 5000.02, *Operation of the Defense Acquisition System*, and as directed by the CA SAPCO, resource and appoint an ISSE in writing to ensure:
    - The system is designed, developed, and implemented with required security features and safeguards;
    - Enhancements to existing systems provide equal or improved security features and safeguards;

f. Coordinate with the AO to ensure the appropriate SCA (or other AO designee) is identified as early as possible for ongoing coordination on security decisions. SCA participation is most important at the Preliminary Design Review (PDR) and the Critical Design Review (CDR). This will ensure systems are fielded or modified within acceptable risk parameters and the latest security technology is being incorporated into system designs;

g. Ensure the Configuration Management (CM) process is addressed and used when new IS are under development, being procured, or delivered for operation. CM is an integral part of the system authorization process. Therefore, it is imperative that the AO/DAO be advised of CM decisions;

h. Ensure all information systems acquisitions (to include weapon systems) remain compliant with IA and technology acquisition requirements as depicted in DoD Directive (DoDD) 5000.01, *The Defense Acquisition System,* and DoDI 5000.02, *Operation of the Defense Acquisition System*;

i. 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;

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

k. Ensure all steps involved in the acquisition and delivery of an IS are followed. These include, but are not limited to:
    - Clearly describe the IS mission;
    - Formulate a concept and design for meeting the security requirements;
    - Incorporate security requirements during system development;
    - Evaluate interoperability with other systems;

l. Produce/develop security documentation (SSP, POA&M, Security Assessment Plan, etc.) as input to the Security Authorization Package and submit package to the AO via the SCA;
m. Coordinate a Security Assessment schedule with the SCA; and
n. Ensure the POA&M is updated to describe the planned tasks for correcting identified weaknesses within the established timeframes and address any residual findings.

1.5.13 Information System Security Engineer (ISSE)

An ISSE is an individual or group responsible for conducting information system security engineering activities. Information system security engineering is a process that captures and refines information security requirements and ensures that the requirements are effectively integrated into information systems through purposeful security architecting, design, development, and configuration. The ISSE is an integral part of the development team designing and developing organizational information systems or upgrading legacy systems. The ISSE employs best practices when implementing security requirements within an information system including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques.

The ISSE shall be appointed in writing and shall ensure the information system is designed, developed, and implemented with required security features and safeguards. If the ISSM/ISSO is identified to fulfill the role of ISSE, their appointment letter will reflect this and they will fulfill the tasks outlined for the ISSE in addition to the tasks assigned to an ISSM/ISSO.

Reference 2.3.1, RMF Step 1, for when an ISSE is required and who can fulfill those roles. Some organizations also refer to an ISSE as an Information Security Architect or Information Assurance Systems Architect and Engineer (IASAE).

1.5.14 Information System Security Manager (ISSM)

An ISSM is an individual who serves as a principal advisor on all matters, technical and otherwise, involving the security of information systems under his/her purview. The ISSM shall be appointed in writing by their respective chain of command/leadership (e.g., Commander, Commanding Officer, PM, CIO, PSO, or corporate equivalent). When circumstances warrant, a single individual may fill both the ISSM and the ISSO roles. ISSM responsibilities should not be assigned as collateral duties. The ISSM must retain a copy of his/her appointment letter.

Responsibilities of an ISSM include, but are not limited to:

a. Develop and maintain a formal IS security program and policies for their assigned area of responsibility;
b. Develop and oversee operational information systems security implementation policy and guidelines;
c. Coordinate with PSO or cognizant security official on approval of external information systems (e.g., guest systems, interconnected system with another organization);
d. Ensure ISSOs under their purview are appointed in writing and provide oversight to ensure ISSOs follow established IS policies and procedures;
e. The ISSM shall assume ISSO responsibilities in the absence of the ISSO;
f. Maintain required IA certifications;
g. Ensure System Administrators (SA) monitor all available resources that provide warnings of system vulnerabilities or ongoing attacks;
h. Ensure periodic testing is conducted to evaluate the security posture of IS by employing various intrusion/attack detection and monitoring tools (shared responsibility with ISSOs);

i. Ensure all ISSOs receive the necessary technical and security training (e.g., operating system, networking, security management) to carry out their duties;
j. Ensure approved procedures are used for sanitizing and releasing system components and media;
k. Maintain a repository of all organizational or system-level cybersecurity-related documentation (including ATOs) for IS under their purview;
l. Coordinate IS security inspections, tests, and reviews;
m. Ensure proper measures are taken when an IS incident or vulnerability is discovered;
n. Ensure data ownership and responsibilities are established for each IS, and specific requirements (to include accountability, access and special handling requirements) are enforced;
o. Ensure development and implementation of an effective IS security education, training, and awareness program;
p. Ensure CM 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;
q. Serve as a voting member of the Configuration Control Board (CCB) and/or the Risk Executive Board, 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;
r. Maintain a working knowledge of system functions, security policies, technical security safeguards, and operational security measures;
s. Manage, maintain, and execute the information security continuous monitoring plan;
t. Ensure a record is maintained of all security-related vulnerabilities and ensure serious or unresolved violations are reported to the AO/DAO; and
u. Assess changes to the system, its environment, and operational needs that could affect the security authorization.

1.5.15 Information System Security Officer (ISSO)

An ISSO is an individual responsible for ensuring the appropriate operational security posture is maintained for an information system and as such, works in close collaboration with the ISSM and ISO. The ISSO shall be appointed in writing by the authority at a site responsible for information system security (e.g., ISSM, Commander, Commanding Officer, PM, CIO, PSO, or corporate equivalent). The ISSO shall have the detailed knowledge and expertise required to manage the security aspects of an information system 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 and ISO, 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. Assist the ISSM in meeting their duties and responsibilities. The ISSO shall assume ISSM responsibilities in the absence of the ISSM;
b. Ensure systems are operated, maintained, and disposed of in accordance with security policies and procedures as outlined in the security authorization package;
c. Attend required technical and security training (e.g., operating system, networking, security management) relative to assigned duties;

d. Maintain required IA certifications;
e. 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;
f. Report all security-related incidents to the ISSM;
g. Conduct periodic reviews of information systems to ensure compliance with the security authorization package;
h. Serve as member of the CCB, if designated by the ISSM;
i. Coordinate any changes or modifications to hardware, software, or firmware of a system with the ISSM and AO/DAO prior to the change;
j. Formally notify the ISSM and AO/DAO when changes occur that might affect system authorization;
k. Monitor system recovery processes to ensure security features and procedures are properly restored and functioning correctly;
l. Ensure all IS security-related documentation is current and accessible to properly authorized individuals; and
m. Ensure audit records are collected, reviewed, and documented (to include any anomalies).

1.5.16 Privileged Users

See Account Management [AC-2], Separation of Duties [AC-5] and Rules of Behavior [PL-4], for privileged user responsibilities and considerations when appointing individuals to this role.

1.5.17 General Users

See Account Management [AC-2] and Rules of Behavior [PL-4], for general user responsibilities.

1.6 DOCUMENT ORGANIZATION AND USE

The remainder of this document is organized as follows:

- **Chapter 2** provides an introduction to the RMF, a discussion of the fundamentals of the RMF and a description of the six steps comprising the RMF, namely: Categorize, Select, Implement, Assess, Authorize, and Monitor.
- **Chapter 3** provides policy and procedures for the DoD SAP Community and for all information systems under the purview of the cognizant SAP AO as they relate to each of the eighteen (18) security control families defined in NIST SP 800-53 and the eight (8) privacy control families defined in the same document.
- **Supporting appendices** provide additional information regarding the application of the JSIG. These include:
    - **Appendix A**: References
    - **Appendix B**: Acronyms
    - **Appendix C**: SAP Security Control Baselines
    - **Appendix D**: Confidentiality Impact Level Flowchart
    - **Appendix E**: Definitions

The JSIG is intended for use by all personnel with a responsibility for protecting the confidentiality, integrity, and availability of DoD SAP information, information systems, and networks. Table 1-2 provides suggested usage for those roles anticipated to be the primary users of this document. Templates for most of the documents required for a security authorization package, as well as additional resources and tools, are posted to the JAFAN Community Website, an IA-focused site restricted to individuals supporting the DoD SAP Community.

Role	Suggested Focus Areas
AO/DAO	Primarily Chapters 1 and 2
SCA	Entire document with emphasis on Chapters 2, 3, and Appendix C
ISO	Entire document with emphasis on Chapters 2, 3, Appendix C, and JSIG templates
ISSE	Entire document with emphasis on Chapters 2, 3, Appendix C, and JSIG templates
ISSM/ISSO	Entire document with emphasis on Chapter 3
Privileged User	References for specific topics, e.g., Account Management [AC-2] and Audit (AU)
General User	Trained in accordance with JSIG; no direct usage

Table 1-2: Suggested Usage of this Document by Role

2 RISK MANAGEMENT FRAMEWORK (RMF)

2.1 Introduction to the RMF

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

- Building information security capabilities into federal information systems through the application of community best practices for management, operational, and technical security controls;
- Maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes; and
- 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 information systems.

The six-step RMF is depicted in Figure 2-1. The RMF steps include:

1. **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.
2. **Select** an initial set of baseline security controls for the IS based on the security categorization; apply overlay(s), if applicable; then tailor the security control baseline as needed based on an organizational assessment of risk and local conditions.
3. **Implement** the security controls and describe how the controls are employed within the IS and its environment of operation.
4. **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.
5. **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.
6. **Monitor** the security controls in the IS on an ongoing basis to include 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.

Figure 2-1: Risk Management Framework (RMF)

Each RMF step includes associated tasks to be carried out by the appropriate organization or individual. These steps and the tasks associated with them, as they apply to the DoD SAP Community and to all IS under the purview of the cognizant SAP AO, are described briefly in Section 2.3. For additional details regarding RMF, see NIST SP 800-37.

2.2 FUNDAMENTALS OF THE RMF

2.2.1 Organization-Wide Risk Management

Managing information system-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. Figure 2-2 illustrates a three-tiered approach to risk management that addresses risk-related concerns at the organization level, the mission and business process level and the information system level. Risk assessments, as described in NIST SP 800-30, provide critical details that guide and inform the security control selection process.

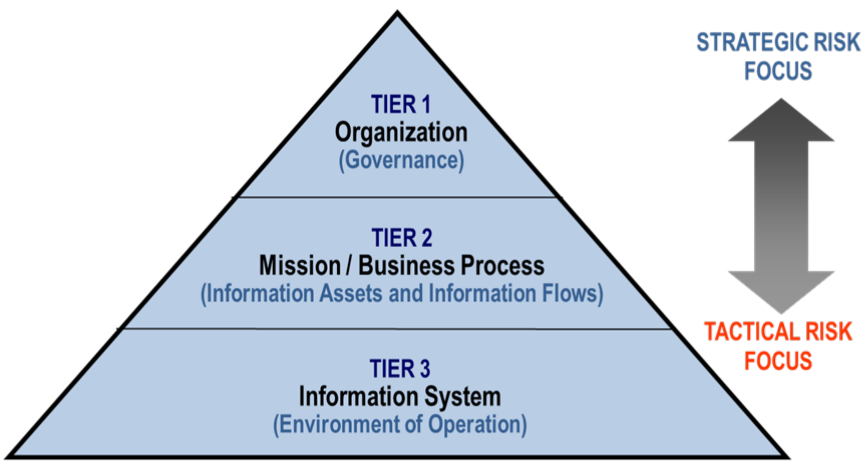


Figure 2-2: Tiered Risk Management Approach

Tier 1 addresses risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy. For the DoD SAP Community, this includes governance provided by the DoD, DoD SAPCO and respective Service/Agency SAPCOs and includes the:

- Techniques and methodologies the organization plans to employ to assess information system-related security risks and other types of risk of concern to the organization;
- Methods and procedures the organization plans to use to evaluate the significance of the risks identified during the risk assessment;
- Types and extent of risk mitigation measures the organization plans to employ to address identified risks;
- Level of risk the organization is willing to accept (i.e., risk tolerance);
- Organization's plans to monitor risk on an ongoing basis given the inevitable changes to organizational information systems and their environments of operation; and

- Degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out.

Tier 2 addresses risk from a mission and business process perspective and is guided by the risk decisions at Tier 1. Tier 2 activities are closely associated with enterprise architecture, to include Wide Area Network (WAN) services (i.e., backbone communications), enterprise services (such as audit reduction tools, network monitoring tools, identity management systems), and services provided across a site/campus (e.g., physical and personnel security). Because subordinate organizations responsible for carrying out derivative or related missions and business processes may have already invested in their own methods of assessing, evaluating, mitigating, accepting and monitoring risk, parent organizations may allow a greater degree of autonomy within parts of the organization or across the entire organization in order to minimize costs. When a diversity of risk assessment methods is allowed, organizations may choose to employ, when feasible, some means of integration of the risk-related information to ensure that the output of the different risk assessment activities can be correlated in a meaningful manner.

Tier 3 addresses risk from an information system perspective and is guided by the risk decisions at Tiers 1 and 2. Risk decisions at Tiers 1 and 2 impact the ultimate selection and deployment of needed safeguards and countermeasures (i.e., security controls) at the information system level. Information security requirements are satisfied by the selection and successful implementation of appropriate management, operational, and technical security controls from NIST SP 800-53. For all DoD SAP information systems under the purview of the cognizant SAP AO, security control selection is guided by the RMF process as directed by DoDM 5205.07, *DoD SAP Security Manual,* and described in the JSIG (i.e., this document) in Section 2.3 below.

2.2.2 System Development Life Cycle (SDLC)

All federal information systems, including operational systems, systems under development, and systems undergoing modification or upgrade, are in some phase of a SDLC. NIST identifies five phases of a general SDLC as Initiation, Acquisition/Development, Implementation/Assessment, Operations/Maintenance, and Disposition/Sunset. Risk management tasks begin early in the SDLC and are important in shaping the security capabilities of the information system. If these tasks are not adequately performed during the initiation, development, and acquisition phases of the SDLC, the tasks will, by necessity, be undertaken later in the life cycle and be more costly to implement. In either situation, all tasks must be completed prior to placing the information system into operation, or continuing its operation, to ensure that information system-related security risks are adequately addressed on an ongoing basis and that the AO explicitly understands and accepts the risk to organizational operations and assets, individuals, other organizations, and national security based on the implementation of the defined set of security controls and the current security state of the information system.

Requirements definition is a critical part of any system development process and begins very early in the life cycle, typically in the initiation phase. Security requirements are a subset of the overall functional and nonfunctional (e.g., quality, assurance) requirements levied on an information system and are incorporated into the SDLC simultaneously with the functional and nonfunctional requirements. Without the early integration of security requirements, significant expense may be incurred by the organization later in the life cycle to address security considerations that could have been included in the initial design. When security requirements are considered as an integral subset of other information system requirements, the resulting system has fewer weaknesses and deficiencies, and therefore fewer vulnerabilities that can be exploited in the future.

Early integration of information security requirements into the SDLC is the most cost-effective and efficient method for an organization to ensure that its protection strategy is implemented. It also ensures that information security processes are not isolated from the other routine management processes employed by the organization to develop, implement, operate, and maintain information systems supporting ongoing missions and business functions. In addition to incorporating information security requirements into the SDLC, security requirements are also integrated into the program, planning, and budgeting activities within the organization to ensure that resources are available when needed and program/project milestones are completed in accordance with the agreed-upon schedule.

Organizations should maximize the use of security-relevant information (e.g., assessment results, information system documentation, and other artifacts) generated during the SDLC to satisfy requirements for similar information needed for information security-related purposes. The reuse of security-relevant information by organizations is an effective method to help eliminate duplication of effort, reduce documentation, promote reciprocity, and avoid unnecessary costs that may result when security activities are conducted independently of system development life cycle processes. In addition, reuse promotes greater consistency of information used in the design, development, implementation, operation, maintenance, and disposition of an information system including security-related considerations.

Throughout the SDLC system owners must be cognizant of changes to the system, documenting and following a change control process to ensure configuration management. Since systems routinely experience changes over time to accommodate new requirements, new technologies or new risks, they must be routinely analyzed in respect to the security posture. All changes shall be captured, approved by the AO as required, and documented in the SSP. Major or significant changes may require re-authorization of the system.

The figure below, from DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, depicts the alignment of RMF steps with the DoD Acquisition Management System, which is explained in DoDI 5000.02, *Operation of the Defense Acquisition System*.

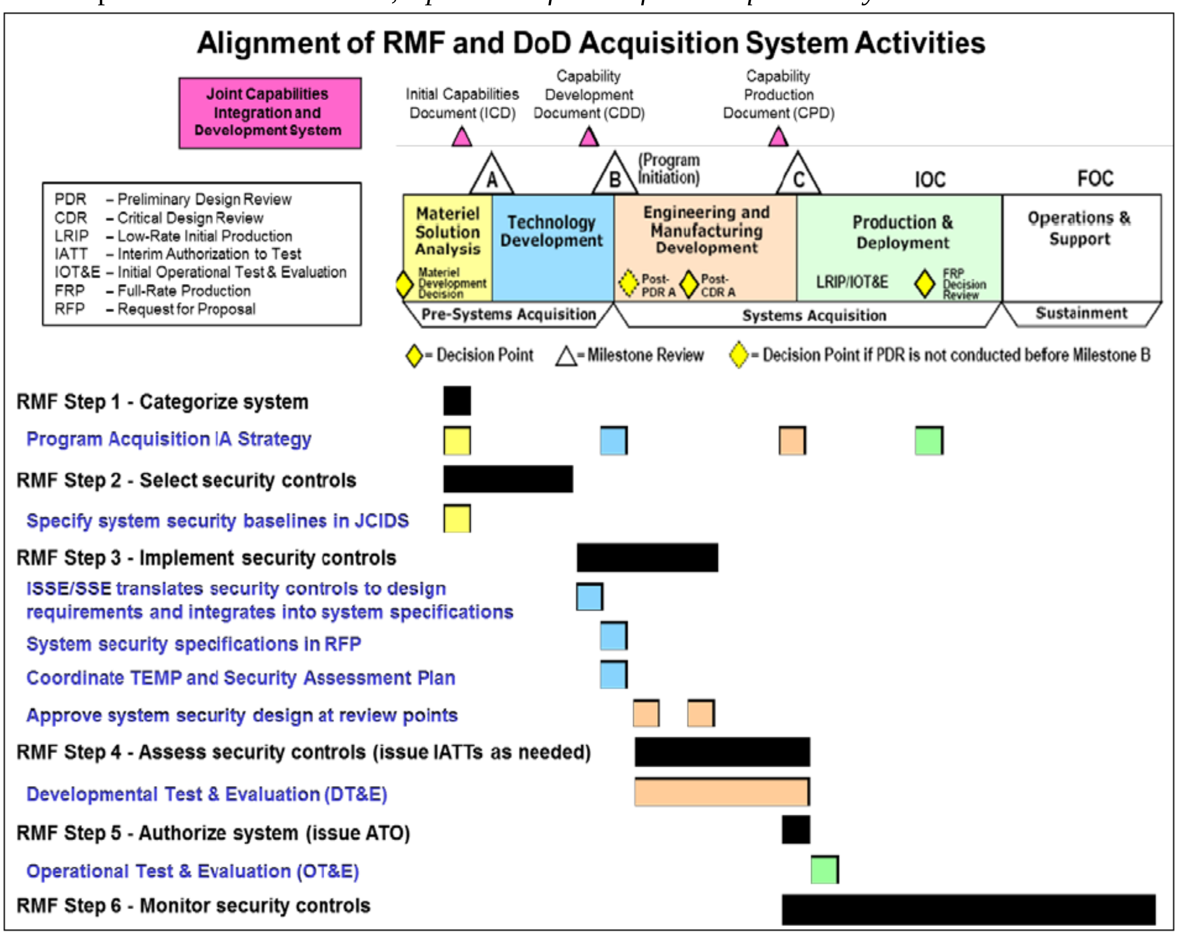


Figure 2-3: Alignment of RMF and DoD System Acquisition Activities

2.2.3 Information System Boundaries

One of the most challenging problems for the ISO, AO, CIO, CISO, ISSM/ISSO, and ISSE is identifying appropriate boundaries for information systems. With regard to the risk management process and information security, the term information system boundary is synonymous with authorization boundary. Well-defined boundaries establish the scope of protection for information systems (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. Information system boundaries are established in coordination with the security categorization process and before the development of the SSP. Information system 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 information systems that must be separately managed and as a consequence, unnecessarily inflate the total information security costs for the organization.

2.2.3.1 Establishing Information System Boundaries

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

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

Since commonality can change over time, the determination of the information system boundary should be revisited periodically as part of the organization's continuous monitoring process. While the above considerations may be useful to organizations in determining information system boundaries for purposes of risk management, they are not viewed as limiting the organization's flexibility in establishing commonsense boundaries that promote effective information security within the available resources of the organization. Information system owners shall consult with key participants, (e.g., AO, CIO, CISO, ISSE, the REF, and other individuals with a vested interest) when establishing or changing system boundaries. The process of establishing information system 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 information system boundary is set, any interconnections with systems outside of that authorization boundary that are approved by a different AO are governed by Interconnection Security Agreements (ISA).

2.2.3.2 Boundaries for Complex Information Systems

The application of security controls within a complex information system can present significant challenges to an organization. From a centralized development, implementation, and operations perspective, the ISO, in collaboration with the AO, CISO, and ISSE, examines the purpose of the information system and considers the feasibility of segmenting the complex system into more manageable subsystems. From a distributed development, implementation, and operations perspective, the organization recognizes that multiple entities, possibly operating under different policies, may be contributing to the development, implementation, and/or operations of the subsystems that compose the complex information system. In such cases, the organization is responsible for ensuring that these separate subsystems can work together in both a secure and functional manner. Treating an information system as multiple subsystems, each with its own subsystem boundary, facilitates a more targeted application of security controls to achieve adequate security and a more cost-effective risk management process. Knowledge of the security properties of individual subsystems does not necessarily provide the complete knowledge of the security properties of the complex information system. The organization applies best practices in systems and security engineering and documents the segmentation of the information system in the SSP.

Information security architecture plays a key part in the security control selection and allocation process for a complex information system. 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 information systems 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 information system, 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 information system level.

2.2.3.3 External Information Systems

External information systems, formerly known as guest systems, are information systems or components of information systems that are outside the authorization boundary of the organization and for which the organization has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. An external information system may be a standalone or an interconnected system/service.

If the system is authorized by an organization other than the Special Access Program Facility's (SAPF) cognizant security authority (CSA) organization, it is an external information system. The PSO, government SAP security officer (GSSO) and/or contractor PSO (CPSO), as appropriate for the SAPF, with ISSM/ISSO coordination, provide written approval of the entry of the external information system into the SAPF. (Reference AC-20)

2.2.3.4 Information Assurance Standard Operating Procedures (IA SOP)

The IA SOP, formerly referred to as a Master SSP (MSSP), provides guidance for the management, use, protection, dissemination, and transmission of program data as it relates to an information system within a SAPF. It is frequently used where the IA-related processes (e.g., configuration management, incident response, media handling, hardware acquisition, movement, and release) are standardized for multiple systems throughout the facility, site or campus. The IA SOP augments the Facility SOP by providing comprehensive procedures and baseline standards for all IA-related processes and procedures. Where a process may deviate from the norm (as described in the IA SOP) for a particular system, the system specific process is captured in that system's SSP.

AO approval of an IA SOP implies general approval of the processes and procedures captured; it does not imply approval of an information system. An SSP specific to a system is required, denoting in the document where a process or procedure is addressed in the IA SOP. The IA SOP must accompany the

SSP as part of the security authorization package requesting an ATO from the AO. Ensure an ATO is granted for each system prior to processing on the system.

2.3 RMF SIX-STEP PROCESS

The RMF and associated RMF tasks apply to both ISOs and common control providers. In addition to supporting the authorization of an IS to operate, the RMF tasks support the categorization of the IS, and the selection, implementation, assessment, and ongoing monitoring of security controls for each IS. Many of the security controls applicable to a system are common controls that are inheritable by the system.

The RMF is life cycle-based; therefore, organizations will need to revisit various tasks over time depending on how the organization manages changes to its information systems and the environment in which those systems operate. Managing information security-related risks for an information system 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 information systems and the flexibility and agility to support the core missions and business operations of the organization in a highly dynamic environment of operation.

The six RMF steps and the tasks associated with them, as they apply to DoD SAP systems and all other systems under the purview of the cognizant SAP AO, are described in the sections that follow.

2.3.1 RMF Step 1, Categorize

Step 1 of the RMF focuses on categorizing the IS. Information systems shall be categorized based on the impact due to a loss of confidentiality, integrity, and availability of the information or information system.

With approval of the cognizant SAP AO, the ISO of a legacy IS in coordination with the SCA will determine the categorization of the IS prior to its transition to RMF. For all information systems - legacy, initial development, or major revision, the ISO shall assign an ISSE at program inception, where required by the AO. The ISSE level of expertise required is dependent on the size and complexity of the IS. The ISSE could be a dedicated role on a large, complex system or the ISSE could oversee several smaller, less complex systems. The function of ISSE could also be performed by the ISSM/ISSO on smaller, less complex systems. This decision is made by the cognizant SAP AO after discussions with the ISO and ISSM/ISSO.

The ISO, in conjunction with the ISSM/ISSO and ISSE, is responsible for the following tasks when categorizing the information system:

- **Task 1-1**: Categorize the information system and document the results in the SSP.

Each IS shall be categorized by defining the impact levels that would result from a loss of confidentiality, integrity, and availability as indicated in CNSSI 1253, section 3.1:

> Security categorization is a two-step process:
>
> Step 1. Determine impact values for (i) information type(s) processed, stored, transmitted, or protected by the system; and (ii) for the information system.
>
> Step 2. Identify overlays that apply to the IS and its operating environment to account for additional factors.

Potential impact determination for information types required for Step 1 above is further explained in Section 3.1.1 of CNSSI 1253. Additional factors that may raise the impact level of system categorization higher than any impact level assigned to the information types include aggregation of data and critical system functionality. Reference NIST SP 800-60 Vol I, Section 4.4.2 for additional guidance.

Identifying an applicable overlay during RMF Step 1-Categorize, ensures the system categorization is based on an accurate authorization boundary and that appropriate terms are used in the description, e.g., standalone, Cross Domain Solution (CDS). The Classified Overlay applies to all classified NSS including DoD SAP IS and is considered part of the JSIG baseline control set.

The security categorization process is initiated by the ISO who, in coordination with the information owner/steward, proposes the initial impact levels. Security impact levels are defined as low, moderate or high for each of the three security objectives (i.e., confidentiality, integrity, and availability). For example, an information system 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 SCA will review the proposed security impact levels and provide recommendations to the AO. Security impact levels are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

The following paragraphs provide guidance in defining impact levels for all information systems under the purview of the cognizant SAP AO with additional amplification of the terms limited, serious, and severe relative to impact levels provided in Section 2.3.1.4.

2.3.1.1 Confidentiality

The confidentiality impact level for all SAP systems shall be moderate or high. The confidentiality impact level is:

- **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.
- **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.

In addition to the above guidance, the adjustments shown in Table 2-1 shall be applied when defining the confidentiality impact level for Special Access Required (SAR) data. Reference the Confidentiality Impact Level Flowchart in Appendix D for Secret (S) and Top Secret (TS) SAR to determine the confidentiality impact level and applicable overlays as discussed in Section 2.3.1.5 Overlays.

Classification	Confidentiality Impact Level	Adjustments to Impact Level
TS//SAR OR S//SAR	Moderate	Adjust to the high confidentiality impact level if: - Any user lacks either the required security clearance (address with overlay) or the required citizenship

Table 2-1: Confidentiality Impact Level Adjustments

2.3.1.2 Integrity

The integrity impact level is:

- **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.
- **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.
- **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.

2.3.1.3 Availability

The availability impact level is:

- **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., limited impact if system is down more than 24 hours).
- **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., serious impact unless system is up in less than 24 hours).
- **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., severe impact unless system is up within x_minutes).

2.3.1.4 Amplification

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

- A **limited** adverse effect means that, for example, the loss of confidentiality, integrity, or availability 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.
- A **serious** adverse effect means that, for example, the loss of confidentiality, integrity, or availability 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.
- A **severe or catastrophic** adverse effect means that, for example, the loss of confidentiality, integrity, or availability 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.

2.3.1.5 Overlays

Table 2-2 below provides additional guidance for adjusting the overall security categorization levels through the use of overlays. An overlay is a predefined control set which modifies or enhances the baseline controls and targets specific data sets (e.g., personally identifiable information (PII) or privacy data), system type (e.g., CDS, platform IT (PIT)), and/or environment (e.g., space, tactical).

Accessibility Scenario	Apply…
All users have all required clearances, formal access approvals and the need to know for all information on the system.	JSIG Baseline (Appendix C)
All users have all required clearances, formal access approvals and the need to know for some of the information on the system	JSIG Baseline (Appendix C)
At least one user lacks at least one required formal access approval for access to all of the information on the system	JSIG Baseline (Appendix C) + appropriate overlay or tailoring
There is a validated requirement to provide an access, transfer or multi-level CDS	Cross Domain Overlay
PII, as defined by the organization's Privacy Control Officer or AO, is stored on the IS	Privacy Overlay, use low impact level unless otherwise instructed by AO/SCA or Privacy Control Officer

Table 2-2: Overlay Applicability

Additional overlays may be available specific to a system or environment, check with your AO.

- **Task 1-2:** Describe the IS (including system boundary) and document the description the SSP. System may be defined, for example, as a local area network (LAN), wide area network (WAN), standalone, controlled interface (CI), cross domain solution (CDS), platform IT (PIT), or application)
- **Task 1-3:** Register the information system with the appropriate SAP Service/Agency AO or designee. The registration establishes the relationship between the information system and the governing organization of that system and results in the formal assignment of a SCA for the information system.
- **Output from Step 1**
  - Draft SSP
  - System registration

Ideally, a risk assessment is conducted before or during this step and documented in a Risk Assessment Report (RAR) to begin identifying risks to the system.

2.3.2 RMF Step 2, Select

Step 2 of the RMF focuses on selecting the security controls applicable to the information system. The ISO, along with assistance from the ISSE and/or ISSM/ISSO, is responsible for the following tasks:

- **Task 2-1:** Identify the security controls that are provided by the organization as common controls for all or multiple information systems under the organization's control and document the controls in a security plan. Control implementation can be characterized 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 ISO. Common controls are security controls that are inheritable by one or more organizational information systems 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 ISO. Security controls shall be documented in the SCTM, which is a component of the SSP. ISOs should reference the governing source that documents the implementation of the common (i.e., inherited) controls.
- **Task 2-2:** Select the security controls for the information system and document the controls in the security plan. SAP systems utilize the CNSSI 1253 methodology for Security Control Selection (Section 3.2, RMF Step 2, Task 2-2) into two steps: select the initial security control set and tailor the initial security control set.
    1. Select the initial security control set
        - Select the baseline security controls identified from JSIG Appendix C, which includes the Classified Overlay security controls and SAP defined organization values, corresponding to the security category of the system (i.e., the impact values determined for each security objective [confidentiality, integrity, and availability]).
        - Apply any overlay(s) identified as applicable during security categorization. If the use of multiple overlays results in conflicts between the application or removal of security controls, the AO (or designee), in coordination with the information owner/steward, information system owner, and risk executive (function) resolves the conflict.
        - Document the initial security control set and the rationale for adding or removing security controls from the baseline by referencing the applicable overlay(s) in the SCTM as part of the security plan.
    2. Tailor the initial security control set
        - Tailor the initial security control set, including the organization-defined values, as appropriate.
        - Document in the SSP the relevant decisions made during the tailoring process, providing a sound rationale for those decisions.

  Tailoring the controls as needed means to tailor in controls to supplement the set of selected controls, as well as tailor out or modify the controls, as applicable based on the system risk assessment. If a security control identified in the baseline set of controls is tailored out, an explanation must be provided in the SCTM portion of the SSP, describing the rationale as to why the control does not apply or how it is satisfied by other mitigating factors. An explanation must also be provided in the SCTM if an organization-defined value is modified. Security controls may also be added (i.e., tailored in) as necessary depending upon the information system and/or its environment of operation. Ensure the SCA reviews the final set of controls prior to Step 3, Implement.
- **Task 2-3:** Develop a strategy for continuous monitoring of the security control effectiveness. The implementation of a robust continuous monitoring program allows an organization to understand the security state of the information system over time and maintain the initial security authorization in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business functions. Ongoing monitoring of the security controls is a critical part of risk management that must be developed early in the SDLC. Effective monitoring

includes, but is not limited to, configuration management and control, security impact analyses on proposed changes, assessment of selected security controls, and security status reporting.

- **Task 2-4:** Review and approve the SSP. The AO, SCA, or other AO designee, review the SSP to determine if the plan is updated, consistent, meets the established security requirements and identifies potential risks. This task ensures the AO concurs with the ISO on system categorization and control set (baseline, overlay(s), tailoring) relative to the assessed risk. Feedback shall be provided to the ISO, ISSM/ISSO, and ISSE. Any exceptions to the baseline controls and overlay controls must be approved by the AO.
- **Output from Step 2**
  - Updated draft SSP/SCTM
  - Draft Risk Assessment Report (RAR)
  - Documented Continuous Monitoring (ConMon) Plan/Strategy
  - Approved draft SSP/SCTM

2.3.3 RMF Step 3, Implement (Develop/Build)

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

- **Task 3-1:** Implement the security controls specified in the SSP.
- **Task 3-2:** Document the security control implementation in the SCTM portion of 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. The level of effort expended on documentation of the information system is commensurate with the purpose, scope, and impact of the system with respect to organizational missions, business functions, and operations.
- **Output from Step 3**
  - Updated SSP/SCTM

2.3.4 RMF Step 4, Assess (Test)

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

- **Task 4-1:** Develop, review, and approve a plan to assess the security controls.

  The ISO, in conjunction with the ISSM/ISSO or ISSE, shall develop a plan to assess the security controls. The Security Assessment Plan shall provide the objectives for the security control assessment, the proposed method for verifying compliance with security controls, a proposed schedule for conducting the assessment, and assessment procedures. The assessment plan will be reviewed by the SCA to ensure the plan is consistent with the security objectives of the organization; employs state-of-the-practice tools, techniques, procedures, and automation to support the concept of continuous monitoring and near real-time risk management; and is cost-effective with regard to the resources allocated for the assessment. The SCA will approve the Security Assessment Plan, which will establish appropriate expectations for the security control assessment, define the level of effort for the assessment and ensure the appropriate level of resources are applied in determining the effectiveness of the security controls.
- **Task 4-2:** Assess the security controls in accordance with the security procedures defined in the Security Assessment Plan.

The security assessment, frequently conducted by the SCA, or other AO designee, 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. Additional testing may be conducted at the discretion of the SCA or designee. Some security assessments may require an approval from an AO, depending on data, connections, locations, etc., and the type of testing planned, e.g., interconnections, CDS, penetration testing, etc. An interim authorization to test (IATT) may be requested if, for example, the assessment will include connecting to an operational system, network, or Research Development Test and Evaluation (RDT&E) environment that is already under an authorization to operate (ATO). Additionally, an ISA or authorization to connect (ATC) may be required when connecting a system under assessment to an operational infrastructure (e.g., RDT&E network to operational LAN).

- **Task 4-3:** Prepare the Security Assessment Report (SAR) documenting issues, findings and recommendations from the security control assessment as they pertain to the IS. The SAR is written by the individual(s) performing the assessment, frequently the SCA. However, ISSM/ISSOs may use the SAR to document self-assessment results and, at the direction of the AO/SCA, include a SAR in the Security Authorization Package.
- **Task 4-4:** Conduct initial remediation actions based on the findings and recommendations of the SAR and reassess remediated controls, as appropriate.

  The AO/SCA may determine that certain findings are significant and require immediate remediation actions. If weaknesses or deficiencies in security controls are corrected, the remediated controls must be reassessed by the SCA or designee to determine the extent to which the remediated controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the IS. The SAR is updated with the findings from the reassessment, maintaining a copy of the original assessment results. The ISO shall ensure the SSP is updated as appropriate based on the findings of the security control assessment and any remediation actions taken. The updated SSP shall reflect the actual state of the security controls after the initial assessment and any modifications by the ISO, ISSM/ISSO, ISSE, or common control provider in addressing recommendations for corrective actions. At the completion of the assessment step, the SSP will contain an accurate list and description of the security controls implemented, including compensating controls, and a list of residual vulnerabilities. A compensating control is defined in CNSSI 4009 as, “a management, operational, and 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…that provides equivalent or comparable protection for an information system.”

Security control assessments may be carried out during system development, system implementation, and system operation/maintenance (as part of continuous monitoring).

- **Output from Step 4**
  - Security Assessment Plan
  - SAR
  - Updated RAR
  - Updated SSP

2.3.5 RMF Step 5, Authorize (Deploy/Operate)

Step 5 of the RMF focuses on authorizing the information system for operation and includes the following tasks:

- **Task 5-1:** The Plan of Action and Milestones (POA&M) is initiated based on findings and recommendations from the SAR.

The ISO is responsible for updating the POA&M, to include identifying corrective actions, determining resources required, documenting milestone completion dates, and addressing any residual findings. The POA&M shall identify:

- Tasks to be accomplished with a recommendation for completion either before or after information system implementation. This is usually an input provided by the SCA who performed the assessment.
- Resources required to accomplish the tasks.
- Any milestones in meeting the tasks, to include percentage completed.
- Scheduled completion dates for the milestones.

The POA&M is used by the AO to monitor the progress in mitigating any findings.

- **Task 5-2:** Assemble and submit the security authorization package to the AO.

  The security authorization package contains as a minimum the SSP (which includes the SCTM, ConMon Strategy/Plan, and a RAR); the SAR; and the POA&M. Additional bodies of evidence may be required, as directed by the AO. See Risk Assessment (RA) section for further details regarding the Risk Assessment. The ISO is responsible for verifying that the security authorization package is complete and is submitted for final review to the office of the AO. For information systems inheriting common controls for specific security capabilities, the security authorization package for the common controls or a reference to such documentation must also be included in the authorization package. When security controls are provided to an organization by an external provider (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization shall ensure the information needed by the AO to make a risk-based decision is made available by the control provider.

- **Task 5-3:** The AO, or designee, 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.

  Risk assessments (either formal or informal) may be employed to provide additional information on threats, vulnerabilities, and potential impacts as well as the analyses for the risk mitigation recommendations. The REF also provides information to the AO that is considered in the final determination of risk resulting from the operation and use of the IS.

- **Task 5-4:** Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or national security is acceptable.

  The explicit acceptance of risk is the responsibility of the AO. The AO will consider many factors to determine if the risk to organizational operations, organizational assets, 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 information system 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 (ATO, denied authorization to operate (DATO), IATT) conveys the final security authorization decision from the AO to the ISO, PSO and other organizational officials, as appropriate. The authorization decision document contains the following information:

  - Authorization decision
  - Terms and conditions for the authorization

- Authorization duration
    - Time driven – AO may identify an expiration date
    - Ongoing – Requires a robust and mature continuous monitoring plan

  The security authorization decision indicates to the ISO (or other intended officials) whether the system is issued an ATO, IATT, or DATO. The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the ISO or CCP.

- **Output from Step 5**
  - POA&M
  - Security Authorization Package
  - Authorization decision document

2.3.6 RMF Step 6, Monitor

An effective organizational information security program includes a continuous monitoring program integrated into the SDLC in addition to conducting a thorough point-in-time assessment of the deployed security controls. The objective of the continuous monitoring program is to determine if the set of deployed security controls continue to be effective over time in light of the inevitable changes that occur to the system and/or its operational environment.

An effective continuous monitoring program includes:

- Configuration management and control processes for information systems;
- Security impact analyses on proposed or actual changes to information systems and environments of operation;
- Assessment of selected security controls (including system specific, hybrid, and common controls) based on the defined continuous monitoring strategy;
- Security status reporting to appropriate officials; and
- Active involvement by authorizing officials in the ongoing management of information system-related security risks.

Step 6 of the RMF focuses on monitoring the security controls associated with the information system and includes the following tasks:

- **Task 6-1:** Determine the security impact of proposed or actual changes to the IS and its environment of operation.

  Changes to the IS or its environment of operation may affect the security controls currently in place (including system specific, hybrid, and common controls), produce new vulnerabilities in the system, or generate requirements for new security controls that were not needed previously. The ISO ensures proposed or actual changes to an IS or its environment of operation are documented. Assessing the potential impact those changes may have on the security state of the system or the organization is an important aspect of security control monitoring and maintaining the security authorization over time. The security impact analysis determines the extent to which proposed or actual changes to the IS or its environment of operation affect the security state of the system.

  If the results of the security impact analysis indicate that the proposed or actual changes affect the security state of the system, corrective actions must be initiated to include, but not limited to, notifying the SCA of the proposed system changes or actual changes to the environment of operations. The ISO ensures the change, potential impact, and recommended remediation, if applicable, is documented. The SCA will determine required further actions. No security-related changes to the IS or its environment of operation shall be implemented without first consulting with appropriate organizational officials/entities (e.g., CCB, CISO, SCA). In addition, the security authorization package shall be revised and updated as required.

The AO or designee uses the revised and updated SAR to determine if a formal reauthorization action is necessary. Most routine changes to an information system 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.

- **Task 6-2:** Assess a selected subset of the security controls employed within and inherited by the information system 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 ISO or CCP 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:

  - Security control assessments conducted as part of an information system authorization, ongoing authorization, or formal reauthorization.
  - Continuous monitoring activities to include self-assessments and/or security reviews.
  - Testing and evaluation of the information system as part of the system development life cycle process or audit.

  The ISO is responsible for ensuring the results of continuous monitoring activities shall be reported to the AO on an ongoing basis in the form of status reports.

- **Task 6-3:** Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M.

  The ISO ensures remediation activities are conducted and documented as indicated in Task 6-4.

- **Task 6-4**: Update the SSP, SAR, and POA&M based on the results of the continuous monitoring process.

  The ISO shall ensure all relevant documentation is updated. The SSP/SCTM, RAR, and ConMon frequency shall reflect any modifications to security controls based on risk mitigation activities carried out by the ISO or CCP. 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 discovered during the security impact analysis or security control monitoring, and describe how the ISO or CCP 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 the SSP and POA&M, organizations shall ensure that the original information needed for oversight, management, and auditing purposes is not modified or destroyed.

- **Task 6-5:** Report the security status of the IS (including the effectiveness of security controls employed within and inherited by the system) to the AO and other appropriate organization officials on an ongoing basis in accordance with the monitoring strategy.

  The ISO is responsible for reporting the security status of the IS. Reporting can be event driven, time driven or both. The goal is efficient ongoing communication with senior leaders conveying the current security state of the information system and its environment of operation with regard to organizational missions and business functions. Security status reports shall be appropriately marked, protected, and handled in accordance with federal and organizational policies.

- **Task 6-6:** Review the reported security status of IS (including the effectiveness of security controls employed within and inherited by the systems) on an ongoing basis in accordance with the organization's continuous monitoring strategy.

  This review by the AO or designee shall determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or national security remains acceptable. By carrying out ongoing risk determination and risk acceptance, the AO can maintain the security authorization over time.

- **Task 6-7:** Implement an IS decommissioning strategy, when needed, which executes required actions when a system is removed from service.

  The ISO shall ensure that all security controls addressing information system removal and decommissioning (e.g., media sanitization, configuration management and control) are implemented. A retention plan for records associated with the information system must be proposed by the ISO and approved by the AO prior to destruction of the records. 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 ISO shall formally decommission the IS by issuing a Decommission letter.

- **Output from Step 6**
  - Periodic ConMon deliverables
  - Updated SSP, SAR, POA&M
  - Updated Security Authorization, as appropriate

3 POLICY AND PROCEDURES

EXCERPT FROM NIST SP 800-53 REVISION 4 APPENDIX F WITH OVERPRINT GUIDANCE FOR THE SAP COMMUNITY

This chapter provides policy and procedures as they relate to each of the eighteen (18) security control families defined in NIST SP 800-53.

Of the eighteen (18) security control families in NIST SP 800-53, seventeen (17) families are described in NIST SP 800-53, Appendix F; one (1) additional family (Program Management [PM]) is addressed in Appendix G and provides controls for information security programs. The PM family provides security controls at the organizational rather than the information-system level and applies to all impact levels in all baselines. The PM family is not listed in alphabetic order, but follows the SI family in this chapter. In addition to the 18 families, NIST SP 800-53, Appendix J addresses Privacy and identifies an additional 8 control families. Reference the JSIG Chapter 2 discussion on overlays for guidance on Privacy. Each security control family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each security control family. Table 3-1 summarizes the families and the associated security control family identifiers.

AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
PM	Program Management

Table 3-1: Security Control Families and Identifiers

Security controls are identified by appending a numeric identifier to the family identifier to indicate the number of the control within the family. For example, AC-2 is the second control in the Access Control family, and CP-9 is the ninth control in the Contingency Planning family. Some controls have been withdrawn and incorporated into other controls by NIST. Numbers associated with these controls remain within each Security Control Family to maintain the numbering schema used in NIST SP 800-53, but are identified as “withdrawn.” Some controls are not included in any baseline; they may be added in as required by overlay or tailoring requirements.

This chapter of the JSIG is comprised of the catalog of security controls from Appendix F of NIST SP 800-53 Revision 4. The original NIST text is preserved for the security control, control enhancement, and supplemental guidance, where provided. The exception is where the NIST control (including the control enhancement) indicates a requirement for the assignment of an organization-defined parameter value. Where assigned, the JSCS WG (DoD SAP Community) organization-defined value appears in the control text in bold, replacing the original italicized NIST verbiage. CNSSI 1253 defines values for a number of controls requiring an organization-defined value. Where the JSCS WG determined the SAP Community could/should align with the CNSS value, that value was captured in the control text of this JSIG. Where it was determined that the SAP Community was better served by assigning a different or more articulate value, that value appears in the control text in bold replacing the original italicized assignment verbiage as stated above. If the original NIST assignment text is still in place, it was determined that the organization-defined parameter value should be assigned at the organization or system level and not at the SAP Community level. Assignment at the organization or system level provides an opportunity for an organization to tailor the security controls to support specific mission, business, or operational needs. See control AC-5 used as an example below.

AC-5 SEPARATION OF DUTIES

Control ID and Control Title

Control: The organization:

NIST Control Verbiage

NIST Assignment to Organization (italics)

SAP Assigned Organization Value (bold)

a. Separates [*Assignment: organization-defined duties of individuals*]**, at a m administrators shall not also perform security audit administration functions and Media Custodians shall not perform DTA functions without specific AO appr**

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, PE-3, PE-4, PS-2.

NIST Supplemental Guidance

Different privileged accounts should be assigned for different roles. Organizations should separate roles for network or database administration from other sensitive functions, such as cryptographic key management, hardware management, removable media data transfer, system security management, or access to particularly sensitive information.

SAP Supplemental Guidance (text box)

As shown in the example above, SAP guidance for a given control or control enhancement is provided in a textbox and located following the relevant control or control enhancement in the catalog of controls below. The focus for providing additional SAP guidance is on controls that are included in a moderate-low-low (MLL) or moderate-moderate-low (MML) baseline, and only as needed. Not all controls will have a textbox because NIST supplemental guidance frequently provides sufficient guidance.

The AO may authorize or require tailoring of controls based on risks identified to the information, information system and/or its environment of operation. Tailoring may include compensatory measures or manual procedures in lieu of automated/technical solutions. The SSP/SCTM must address those situations where tailoring methods are implemented. Tailoring must be approved in writing by the AO or designee. Tailored controls should be reviewed at least annually as part of the continuous monitoring process.

The JSIG provides policy and procedures within each control family in the sections that follow. Therefore, the JSIG may be cited for compliance with the -1 policy controls for each family in addition to organization, site, and program specific policy. Policy and procedures applicable to multiple systems at a given site/campus may be captured in an IA SOP as required by the respective AO with additional policy and procedures specific to the system captured in the SSP/SCTM. In addition to the JSIG, service/agency specific policies and procedures may be required. Organization-defined parameter values within the JSIG are assigned for the DoD SAP Community through the JSCS WG and are applicable to DoD SAP systems if not otherwise defined by formal organization policy or tailored with AO approval.

FAMILY: ACCESS CONTROL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

   1. Access control policy **annually or as policy and procedures dictate changes are required**; and

   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: PM-9.

DoD SAP-specific policy and procedures related to access control are defined in the remainder of this control family.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

AC-2 ACCOUNT MANAGEMENT

Control: The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: **as defined by the service or program**;

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 **ISO or designee** for requests to create information system accounts;

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with **the service or program policy**;

g. Monitors the use of information system accounts;

h. Notifies account managers:

   1. When accounts are no longer required;

   2. When users are terminated or transferred; and

   3. When individual information system usage or need-to-know changes;

i. Authorizes access to the information system based on:

   1. A valid access authorization;

   2. Intended system usage; and

   3. Other attributes as required by the organization or associated missions/business functions;

j. Reviews accounts for compliance with account management requirements **at least annually**; and

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

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., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. 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, MA-3, MA-4, MA-5, PL-4, SC-13.

Types of Accounts

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 SAP 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 removed within 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 USERID/password for continuing processes under another individual member of a common functional group. Reference IA-2 and IA-2(5).

Control Enhancements:

(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

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

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

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

The information system automatically **disables** temporary and emergency accounts after **not to exceed 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.

(3) ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS

The information system automatically disables inactive accounts after **not to exceed ninety (90) days**.

(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Related controls: AU-2, AU-12.

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

The organization requires that users log out **when user’s work day has ended or there is an extended absence (more than six (6) hours).**

Supplemental Guidance: Related control: SC-23.

(6) ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT

The information system implements the following dynamic privilege management capabilities: [*Assignment: organization-defined list of dynamic privilege management capabilities*].

Supplemental Guidance: In contrast to conventional access control approaches which employ static information system accounts and predefined sets of user privileges, dynamic access control approaches (e.g., service-oriented architectures) rely on run time access control decisions facilitated by dynamic privilege management. While user identities may remain relatively constant over time, user privileges may change more frequently based on ongoing mission/business requirements and operational needs of organizations. Dynamic privilege management can include, for example, the immediate revocation of privileges from users, as opposed to requiring that users terminate and restart their sessions to reflect any changes in privileges. Dynamic privilege management can also refer to mechanisms that change the privileges of users based on dynamic rules as opposed to editing specific user profiles. This type of privilege management includes, for example, automatic adjustments of privileges if users are operating out of their normal work times, or if information systems are under duress or in emergency maintenance situations. This control enhancement also includes the ancillary effects of privilege changes, for example, the potential changes to encryption keys used for communications. Dynamic privilege management can support requirements for information system resiliency. Related control: AC-16.

(7) ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES

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) Takes **the following action: Disables (or revokes) privileged user accounts** when privileged role assignments are no longer appropriate.

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 (DTA).

(8) ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION

The information system creates [*Assignment: organization-defined information system accounts*] dynamically.

Supplemental Guidance: Dynamic approaches for creating information system accounts (e.g., as implemented within service-oriented architectures) rely on establishing accounts (identities) at run time for entities that were previously unknown. Organizations plan for dynamic creation of information system accounts by establishing trust relationships and mechanisms with the appropriate authorities to validate related authorizations and privileges. Related control: AC-16.

(9) ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS

The organization only permits the use of shared/group accounts that meet [*Assignment: organization-defined conditions for establishing shared/group accounts*].

See also supplemental guidance for AC-2.k.

(10) ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION

The information system terminates shared/group account credentials when members leave the group.

See also supplemental guidance for AC-2.k.

(11) ACCOUNT MANAGEMENT | USAGE CONDITIONS

The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [*Assignment: organization-defined information system accounts*].

Supplemental Guidance: Organizations can describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.

(12) ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE

The organization:

a. Monitors information system accounts for [*Assignment: organization-defined atypical use*]; and

b. Reports atypical usage of information system accounts to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Atypical usage includes, for example, accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations. Related control: CA-7.

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

The organization disables accounts of users posing a significant risk within **30 minutes of discovery of the risk**.

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: PS-4.

See also AU-6.

References: None.

AC-3 ACCESS ENFORCEMENT

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

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, PE-3.

> All information systems shall, at a minimum, enforce a discretionary access control (DAC) 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 compartmentalized data as defined by the Data Owner, and CDS. See also Protection of Information at Rest [SC-28], Access Control for Mobile Devices [AC-19], and CDS in Information Flow Enforcement [AC-4].
>
> **Access by Foreign Nationals -** DoD SAP information is not releasable to foreign nationals except as authorized by the respective service/agency SAPCO.

Control Enhancements:

(1) ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS

[Withdrawn: Incorporated into AC-6].

(2) ACCESS ENFORCEMENT | DUAL AUTHORIZATION

The information system enforces dual authorization **for all transfers of data from a classified computer network to 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: CP-9, MP-6.

> 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 Agents (DTAs) are the only individuals authorized to transfer data from a classified system to removable media. Only System Administrators are authorized to enable permissions to transfer removable media.
>
> Media Custodians are not authorized to be DTAs.

(3) ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL

The information system enforces [*Assignment: organization-defined mandatory access control policies*] over all subjects and objects where the policy specifies that:

(a) The policy is uniformly enforced across all subjects and objects within the boundary of the information system;

(b) A subject that has been granted access to information is constrained from doing any of the following;

(1) Passing the information to unauthorized subjects or objects;

(2) Granting its privileges to other subjects;

(3) Changing one or more security attributes on subjects, objects, the information system, or information system components;

(4) Choosing the security attributes and attribute values to be associated with newly created or modified objects; or

(5) Changing the rules governing access control; and

(c) [*Assignment: Organized-defined subjects*] may explicitly be granted [*Assignment: organization-defined privileges (i.e., they are trusted subjects)*] such that they are not limited by some or all of the above constraints.

Supplemental Guidance: Mandatory access control as defined in this control enhancement is synonymous with nondiscretionary access control, and is not constrained only to certain historical uses (e.g., implementations using the Bell-LaPadula Model). The above class of mandatory access control policies constrains what actions subjects can take with information obtained from data objects for which they have already been granted access, thus preventing the subjects from passing the information to unauthorized subjects and objects. This class of mandatory access control policies also constrains what actions subjects can take with respect to the propagation of access control privileges; that is, a subject with a privilege cannot pass that privilege to other subjects. The policy is uniformly enforced over all subjects and objects to which the information system has control. Otherwise, the access control policy can be circumvented. This enforcement typically is provided via an implementation that meets the reference monitor concept (see AC-25). The policy is bounded by the information system boundary (i.e., once the information is passed outside of the control of the system, additional means may be required to ensure that the constraints on the information remain in effect). The trusted subjects described above are granted privileges consistent with the concept of least privilege (see AC-6). Trusted subjects are only given the minimum privileges relative to the above policy necessary for satisfying organizational mission/business needs. The control is most applicable when there is some policy mandate (e.g., law, Executive Order, directive, or regulation) that establishes a policy regarding access to sensitive/classified information and some users of the information system are not authorized access to all sensitive/classified information resident in the information system. This control can operate in conjunction with AC-3 (4). A subject that is constrained in its operation by policies governed by this control is still able to operate under the less rigorous constraints of AC-3 (4), but policies governed by this control take precedence over the less rigorous constraints of AC-3 (4). For example, while a mandatory access control policy imposes a constraint preventing a subject from passing information to another subject operating at a different sensitivity label, AC-3 (4) permits the subject to pass the information to any subject with the same sensitivity label as the subject. Related controls: AC-25, SC-11.

(4) ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL

The information system enforces [*Assignment: organization-defined discretionary access control policies*] over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following:

(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.

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.

The policy shall address at a minimum:

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

(5) ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION

The information system prevents access to [*Assignment: organization-defined security-relevant information*] except during secure, non-operable system states.

Supplemental Guidance: Security-relevant information is any information within information systems that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce system security policies or maintain the isolation of code and data. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Secure, non-operable system states include the times in which information systems are not performing mission/business-related processing (e.g., the system is off-line for maintenance, troubleshooting, boot-up, shut down). Related control: CM-3.

(6) ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION

[Withdrawn: Incorporated into MP-4 and SC-28].

(7) ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL

The information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*Assignment: organization-defined roles and users authorized to assume such roles*].

Supplemental Guidance: Role-based access control (RBAC) is an access control policy that restricts information system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on organizational information systems associated with the organization-defined roles. When users are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a significant number of individuals for mid- to large-size organizations) but are instead acquired through role assignments. RBAC can be implemented either as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3 (3) define the scope of the subjects and objects covered by the policy.

(8) ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS

The information system enforces the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [*Assignment: organization-defined rules governing the timing of revocations of access authorizations*].

Supplemental Guidance: Revocation of access rules may differ based on the types of access revoked. For example, if a subject (i.e., user or process) is removed from a group, access may not be revoked until the next time the object (e.g., file) is opened or until the next time the subject attempts a new access to the object. Revocation based on changes to security labels may take effect immediately. Organizations can provide alternative approaches on how to make revocations immediate if information systems cannot provide such capability and immediate revocation is necessary.

(9) ACCESS ENFORCEMENT | CONTROLLED RELEASE

The information system does not release information outside of the established system boundary unless:

(a) The receiving [*Assignment: organization-defined information system or system component] provides [Assignment: organization-defined security safeguards*]; and

(b) [*Assignment: organization-defined security safeguards*] are used to validate the appropriateness of the information designated for release.

Supplemental Guidance: Information systems can only protect organizational information within the confines of established system boundaries. Additional security safeguards may be needed to ensure that such information is adequately protected once it is passed beyond the established information system boundaries. Examples of information leaving the system boundary include transmitting information to an external information system or printing the information on one of its printers. In cases where the information system is unable to make a determination of the adequacy of the protections provided by entities outside its boundary, as a mitigating control, organizations determine procedurally whether the external information systems are providing adequate security. The means used to determine the adequacy of the security provided by external information systems include, for example, conducting inspections or periodic testing, establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received need not be the same as those used by the organization, but the means employed are sufficient to provide consistent adjudication of the security policy to protect the information. This control enhancement requires information systems to employ technical or procedural means to validate the information prior to releasing it to external systems. For example, if the information system passes information to another system controlled by another organization, technical means are employed to validate that the security attributes associated with the exported information are appropriate for the receiving system. Alternatively, if the information system passes information to a printer in organization-controlled space, procedural means can be employed to ensure that only appropriately authorized individuals gain access to the printer. This control enhancement is most applicable when there is some policy mandate (e.g., law, Executive Order, directive, or regulation) that establishes policy regarding access to the information, and that policy applies beyond the realm of a particular information system or organization.

(10) ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS

The organization employs an audited override of automated access control mechanisms under [*Assignment: organization-defined conditions*].

Supplemental Guidance: Related controls: AU-2, AU-6.

References: None.

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 based on [*Assignment: organization-defined information flow control policies]*.

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 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). AFTs require data tracking logs for all transfers and a trained DTA.

Controlled Interface (CI)

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)

Cross Domain Solution (CDS)
A CDS is a form of controlled interface, utilizing a trusted operating system and enforcing a security policy to provide access to and/or transfer data between different security domains. A CDS requires a higher level of assurance, both from a hardware and software perspective.

In the most simplistic terms a CDS is a set of mechanisms that implement the capabilities to access or transfer information (manually or automatically) between two or more security domains and enforce their security policies. This means the end points of the cross domain interconnections operate under different security policies with regard to classification, access or releasability of information. For example, when two information systems and/or networks of different security domains are connected together enabling access and/or data-flow between them, a CDS is mandatory and placed between the two domains.

A well-designed CDS prevents untrusted and potentially malicious data from entering the network of the higher classification and prevents data of a higher classification from leaking into the network of a lower classification.

The creation, validation (assessment and authorization), and life cycle support of a CDS can be time consuming and resource intensive. In 2006 as a result of urgent operational demands to share information more effectively across security domains throughout the federal government, the DoD and the IC CIOs established an interagency office – the Unified Cross Domain Services Management Office (UCDSMO), which focuses on delivering modern cross domain capabilities to the field.

The primary function of the UCDSMO is to provide centralized coordination and oversight of all cross domain activities and ensure a common approach for the implementation of cross domain capabilities within the DoD and the IC. This means the UCDSMO will provide and maintain a list of supported CDS which are certified and fully documented (body of evidence) and a sunset list of CDS that are at the end of their life cycle. The UCDSMO-supported CDS still require authorization on a case-by-case basis by your respective AO. Contact the AO during initial CDS discussions, i.e., during the Pre-acquisition phase, and prior to engaging the UCDSMO. See AC-4(20)

CDS Types
To help determine what type of CDS is required, the UCDSMO-supported CDS are divided into three functional types:

- Data Transfer Solutions: Used to interconnect networks or information systems that operate in different security domains and transfer information between them.
- Access Solutions: Used to provide simultaneous visualization of information from multiple security domains via a single workstation without any data transfer between the various domains.
- Multi-Level Solutions: Used to store data in multiple security domains at varied security levels and allow users to access the data at an appropriate security level.

A requirement to share information between different security domains requires AO coordination for selection, authorization, and connection approval.

Assured File Transfers (AFT)
There are two types of data transfers: Low-to-High and High-to-Low. Documented and AO approved data transfer procedures are required for both types.

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, e.g., S//SAR-A/SAR-B/SAR-C to S//SAR-A/SAR-B/SAR-C.

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, between TS//SAR-A/SAR-B/SAR-C and TS//SAR-A/SAR-B/SAR-J.

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. 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 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 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:

- Log for transfers from a lower classified system (Secret or Top Secret) to a higher classified system, e.g., Secret to Top Secret or S//SAR-A/SAR-B to S//SAR-A/SAR-B/SAR-C. Data transferred from an unclassified system must be logged, e.g., vendor software updates or antivirus definition files from Non-secure Internet Protocol Router Network (NIPRNet).
- Two (2) 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.
- 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 cannot be written to. If the test fails and the media is written to on the High side, then 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 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.

- Documented mission justification.
- As a community best practice, use of an automated review tool in lieu of a manual transfer process (e.g., checklist).
- AO approval for use of automated tools or a manual transfer process/checklist.
- A PSO approved key word list.

AFT tools should not be confused with forensic tools. Forensic tools are 'discovery' tools designed for investigation and recovery (e.g., hard drive data), while keeping the files forensically sound and unchanged. An AFT tool performs a deep file inspection into the many complex layers and, in the case of Microsoft Office, the nearly 100 areas where MS Office products store data within a file, also known as metadata. The tool then provides the SME with a 'what you see is what you get' or WYSIWYG view. In addition, the AFT tools address cropped, resized, and hidden images and graphics through a cleansing/flattening/resolution process. AFT tools identify the exact location (page/ paragraph) of keyword hits and cropped/resized graphics. Forensic tools find images and graphics as well as keywords, but do not identify their location, nor do they indicate if an image/graphic was cropped, resized, or hidden.

Control Enhancements:

(1) INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY ATTRIBUTES

The information system uses [*Assignment: organization-defined security attributes*] associated with [*Assignment: organization-defined information, source, and destination objects*] to enforce [*Assignment: organization-defined information flow control policies*] as a basis for flow control decisions.

Supplemental Guidance: Information flow enforcement mechanisms compare security attributes associated with information (data content and data structure) and source/destination objects, and respond appropriately (e.g., block, quarantine, alert administrator) when the mechanisms encounter information flows not explicitly allowed by information flow policies. For example, an information object labeled Secret would be allowed to flow to a destination object labeled Secret, but an information object labeled Top Secret would not be allowed to flow to a destination object labeled Secret. Security attributes can also include, for example, source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit security attributes can be used, for example, to control the release of certain types of information. Related control: AC-16.

(2) INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS

The information system uses protected processing domains to enforce [*Assignment: organization-defined information flow control policies*] as a basis for flow control decisions.

Supplemental Guidance: Within information systems, protected processing domains are processing spaces that have controlled interactions with other processing spaces, thus enabling control of information flows between these spaces and to/from data/information objects. A protected processing domain can be provided, for example, by implementing domain and type enforcement. In domain and type enforcement, information system processes are assigned to domains; information is identified by types; and information flows are controlled based on allowed information accesses (determined by domain and type), allowed signaling among domains, and allowed process transitions to other domains.

(3) INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL

The information system enforces dynamic information flow control based on [*Assignment: organization-defined policies*].

Supplemental Guidance: Organizational policies regarding dynamic information flow control include, for example, allowing or disallowing information flows based on changing conditions or mission/operational considerations. Changing conditions include, for example, changes in organizational risk tolerance due to changes in the immediacy of mission/business needs, changes in the threat environment, and detection of potentially harmful or adverse events. Related control: SI-4.

(4) INFORMATION FLOW ENFORCEMENT | CONTENT CHECK ENCRYPTED INFORMATION

The information system prevents encrypted information from bypassing content-checking mechanisms by [*Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method]*].

Supplemental Guidance: Related control: SI-4.

(5) INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES

The information system enforces [*Assignment: organization-defined limitations*] on embedding data types within other data types.

Supplemental Guidance: Embedding data types within other data types may result in reduced flow control effectiveness. Data type embedding includes, for example, inserting executable files as objects within word processing files, inserting references or descriptive information into a media file, and compressed or archived data types that may include multiple embedded data types. Limitations on data type embedding consider the levels of embedding and prohibit levels of data type embedding that are beyond the capability of the inspection tools.

(6) INFORMATION FLOW ENFORCEMENT | METADATA

The information system enforces information flow control based on [*Assignment: organization-defined metadata*].

Supplemental Guidance: Metadata is information used to describe the characteristics of data. Metadata can include structural metadata describing data structures (e.g., data format, syntax, and semantics) or descriptive metadata describing data contents (e.g., age, location, telephone number). Enforcing allowed information flows based on metadata enables simpler and more effective flow control. Organizations consider the trustworthiness of metadata with regard to data accuracy (i.e., knowledge that the metadata values are correct with respect to the data), data integrity (i.e., protecting against unauthorized changes to metadata tags), and the binding of metadata to the data payload (i.e., ensuring sufficiently strong binding techniques with appropriate levels of assurance). Related controls: AC-16, SI-7.

(7) INFORMATION FLOW ENFORCEMENT | ONE-WAY FLOW MECHANISMS

The information system enforces [*Assignment: organization-defined one-way flows*] using hardware mechanisms.

(8) INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTERS

The information system enforces information flow control using [*Assignment: organization-defined security policy filters*] as a basis for flow control decisions for [*Assignment: organization-defined information flows*].

Supplemental Guidance: Organization-defined security policy filters can address data structures and content. For example, security policy filters for data structures can check for maximum file lengths, maximum field sizes, and data/file types (for structured and unstructured data). Security policy filters for data content can check for specific words (e.g., dirty/clean word filters), enumerated values or data value ranges, and hidden content. Structured data permits the interpretation of data content by applications. Unstructured data typically refers to digital information without a particular data structure or with a data structure that does not facilitate the development of rule sets to address the particular sensitivity of the information conveyed by the data or the associated flow enforcement decisions. Unstructured data consists of: (i) bitmap objects that are inherently non language-based (i.e., image, video, or audio files); and (ii) textual objects that are based on written or printed languages (e.g., commercial off-the-shelf word processing documents, spreadsheets, or emails). Organizations can implement more than one security policy filter to meet information flow control objectives (e.g., employing clean word lists in conjunction with dirty word lists may help to reduce false positives).

(9) INFORMATION FLOW ENFORCEMENT | HUMAN REVIEWS

The information system enforces the use of human reviews for [*Assignment: organization-defined information flows*] under the following conditions: [*Assignment: organization-defined conditions*].

Supplemental Guidance: Organizations define security policy filters for all situations where automated flow control decisions are possible. When a fully automated flow control decision is not possible, then a human review may be employed in lieu of, or as a complement to, automated security policy filtering. Human reviews may also be employed as deemed necessary by organizations.

(10) INFORMATION FLOW ENFORCEMENT | ENABLE / DISABLE SECURITY POLICY FILTERS

The information system provides the capability for privileged administrators to enable/disable [*Assignment: organization-defined security policy filters*] under the following conditions: [*Assignment: organization-defined conditions*].

Supplemental Guidance: For example, as allowed by the information system authorization, administrators can enable security policy filters to accommodate approved data types.

(11) INFORMATION FLOW ENFORCEMENT | CONFIGURATION OF SECURITY POLICY FILTERS

The information system provides the capability for privileged administrators to configure [*Assignment: organization-defined security policy filters*] to support different security policies.

Supplemental Guidance: For example, to reflect changes in security policies, administrators can change the list of "dirty words" that security policy mechanisms check in accordance with the definitions provided by organizations.

(12) INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS

The information system, when transferring information between different security domains, uses [*Assignment: organization-defined data type identifiers*] to validate data essential for information flow decisions.

Supplemental Guidance: Data type identifiers include, for example, filenames, file types, file signatures/tokens, and multiple internal file signatures/tokens. Information systems may allow transfer of data only if compliant with data type format specifications.

(13) INFORMATION FLOW ENFORCEMENT | DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS

The information system, when transferring information between different security domains, decomposes information into [*Assignment: organization-defined policy-relevant subcomponents*] for submission to policy enforcement mechanisms.

Supplemental Guidance: Policy enforcement mechanisms apply filtering, inspection, and/or sanitization rules to the policy-relevant subcomponents of information to facilitate flow enforcement prior to transferring such information to different security domains. Parsing transfer files facilitates policy decisions on source, destination, certificates, classification, attachments, and other security-related component differentiators.

(14) INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTER CONSTRAINTS

The information system, when transferring information between different security domains, implements [*Assignment: organization-defined security policy filters*] requiring fully enumerated formats that restrict data structure and content.

Supplemental Guidance: Data structure and content restrictions reduce the range of potential malicious and/or unsanctioned content in cross-domain transactions. Security policy filters that restrict data structures include, for example, restricting file sizes and field lengths. Data content policy filters include, for example: (i) encoding formats for character sets (e.g., Universal Character Set Transformation Formats, American Standard Code for Information Interchange); (ii) restricting character data fields to only contain alpha-numeric characters; (iii) prohibiting special characters; and (iv) validating schema structures.

(15) INFORMATION FLOW ENFORCEMENT | DETECTION OF UNSANCTIONED INFORMATION

The information system, when transferring information between different security domains, examines the information for the presence of [*Assignment: organized-defined unsanctioned information*] and prohibits the transfer of such information in accordance with the [*Assignment: organization-defined security policy*].

Supplemental Guidance: Detection of unsanctioned information includes, for example, checking all information to be transferred for malicious code and dirty words. Related control: SI-3.

(16) INFORMATION FLOW ENFORCEMENT | INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS

[Withdrawn: Incorporated into AC-4].

(17) INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION

The information system uniquely identifies and authenticates source and destination points by [*Selection (one or more): organization, system, application, individual*] for information transfer.

Supplemental Guidance: Attribution is a critical component of a security concept of operations. The ability to identify source and destination points for information flowing in information systems, allows the forensic reconstruction of events when required, and encourages policy compliance by attributing policy violations to specific organizations/individuals. Successful domain authentication requires that information system labels distinguish among systems, organizations, and individuals involved in preparing, sending, receiving, or disseminating information. Related controls: IA-2, IA-3, IA-4, IA-5.

(18) INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING

The information system binds security attributes to information using [*Assignment: organization-defined binding techniques*] to facilitate information flow policy enforcement.

Supplemental Guidance: Binding techniques implemented by information systems affect the strength of security attribute binding to information. Binding strength and the assurance associated with binding techniques play an important part in the trust organizations have in the information flow enforcement process. The binding techniques affect the number and degree of additional reviews required by organizations. Related controls: AC-16, SC-16.

(19) INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA

The information system, when transferring information between different security domains, applies the same security policy filtering to metadata as it applies to data payloads.

Supplemental Guidance: This control enhancement requires the validation of metadata and the data to which the metadata applies. Some organizations distinguish between metadata and data payloads (i.e., only the data to which the metadata is bound). Other organizations do not make such distinctions, considering metadata and the data to which the metadata applies as part of the payload. All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection.

(20) INFORMATION FLOW ENFORCEMENT | APPROVED SOLUTIONS

The organization employs [*Assignment: organization-defined solutions in approved configurations*] to control the flow of [*Assignment: organization-defined information*] across security domains.

Supplemental Guidance: Organizations define approved solutions and configurations in cross-domain policies and guidance in accordance with the types of information flows across classification boundaries. The Unified Cross Domain Management Office (UCDMO) provides a baseline listing of approved cross-domain solutions.

UCDMO is now Unified Cross Domain Services Management Office (UCDSMO).

(21) INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS

The information system separates information flows logically or physically using [*Assignment: organization-defined mechanisms and/or techniques*] to accomplish [*Assignment: organization-defined required separations by types of information*].

Supplemental Guidance: Enforcing the separation of information flows by type can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths perhaps not otherwise achievable. Types of separable information include, for example, inbound and outbound communications traffic, service requests and responses, and information of differing security categories.

(22) INFORMATION FLOW ENFORCEMENT | ACCESS ONLY

The information system provides access from a single device to computing platforms, applications, or data residing on multiple different security domains, while preventing any information flow between the different security domains.

Supplemental Guidance: The information system, for example, provides a desktop for users to access each connected security domain without providing any mechanisms to allow transfer of information between the different security domains.

References: None.

AC-5 SEPARATION OF DUTIES

Control: The organization:

a. Separates **at a minimum, duties of system administrators from audit administration functions; and duties of DTAs from media custodians**;

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, PE-3, PE-4, PS-2.

Different privileged accounts should be assigned for different roles. Organizations should separate roles for network or database administration from other sensitive functions, such as cryptographic key management, hardware management, removable media data transfer, system security management, or access to particularly sensitive information.

Control Enhancements: None.

References: None.

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.

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 formally trained.

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

The organization explicitly authorizes access to [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*]).

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.

One example of this is authorizing access to specific system endpoints, such as access to USB ports, CD/DVD drives, microphones, and cameras as well as 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.

Ensure media access is audited as indicated in AU-2.a.

This control is non-tailorable for all SAP systems.

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

The organization requires that users of information system accounts, or roles, with access to **privileged functions (except the DTA role)**, use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS

The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for [*Assignment: organization-defined compelling operational needs*] and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

The organization restricts privileged accounts on the information system to **absolute minimum number of privileged users needed to manage the system.**

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.

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.

(6) LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS

The organization prohibits privileged access to the information system by non-organizational users.

Supplemental Guidance: Related control: IA-8.

Reference IA-2 for definition of organizational user.

(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

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.

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.

The Presidential Memo, *National Insider Threat Policy and Minimum Standards for Insider Threat Programs*, November 21, 2012, and DoDD 5205.16, *The DoD Insider*

Threat Program, 30 Sep 2014, require that organizations develop insider threat programs to include reporting the status of privileged users (e.g., total number, additions, deletions) on a quarterly basis.

(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 software.

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.

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).

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 an "su" or "sudo" to root privilege to install applications.

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.

(9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS

The information system audits the execution of privileged functions.

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.

(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.

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.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control: The information system:

a. Enforces a limit of **maximum of three (3)** 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.

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

Control Enhancements:

(1) UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK

[Withdrawn: Incorporated into AC-7].

(2) UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE

The information system purges/wipes information from [*Assignment: organization-defined mobile devices*] based on [*Assignment: organization-defined purging/wiping requirements/techniques*] after **10** consecutive, unsuccessful device logon attempts.

Supplemental Guidance: This control enhancement applies only to mobile devices for which a logon occurs (e.g., personal digital assistants, smart phones, tablets). The logon is to the mobile device, not to any one account on the device. Therefore, successful logons to any accounts on mobile devices reset the unsuccessful logon count to zero. Organizations define information to be purged/wiped carefully in order to avoid over purging/wiping which may result in devices becoming unusable. Purging/wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms. Related controls: AC-19, MP-5, MP-6, SC-13.

References: None.

AC-8 SYSTEM USE NOTIFICATION

Control: The information system:

a. Displays to users **DoD Information Systems Standard 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, and 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 [*Assignment: organization-defined conditions*], 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.

Control Enhancements: None.

In accordance with DoDI 8500.01, *Cybersecurity*, March 14, 2014, Enclosure 3, paragraph 9(1)(d), 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 DoD IS user agreements in accordance with applicable security controls and DoD implementation procedures." The required text for the banner and user agreements is posted to DISA's Information Assurance Support Environment (IASE) website under "DoD Consent Banner" at http://iase.disa.mil.

References: None.

AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION

Control: The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

Supplemental Guidance: This control is applicable to logons to information systems via human user interfaces and logons to systems that occur in other types of architectures (e.g., service-oriented architectures). Related controls: AC-7, PL-4.

Control Enhancements:

(1) PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS

The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

(2) PREVIOUS LOGON NOTIFICATION | SUCCESSFUL / UNSUCCESSFUL LOGONS

The information system notifies the user of the number of **successful logons/accesses; unsuccessful logon/access attempts** during **the period since last successful logon**.

(3) PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES

The information system notifies the user of changes to [*Assignment: organization-defined security-related characteristics/parameters of the user's account*] during **the period since last successful logon**

(4) PREVIOUS LOGON NOTIFICATION | ADDITIONAL LOGON INFORMATION

The information system notifies the user, upon successful logon (access), of the following additional information: [*Assignment: organization-defined information to be included in addition to the date and time of the last logon (access)*]**.**

Supplemental Guidance: This control enhancement permits organizations to specify additional information to be provided to users upon logon including, for example, the location of last logon. User location is defined as that information which can be determined by information systems, for example, IP addresses from which network logons occurred, device identifiers, or notifications of local logons.

References: None.

AC-10 CONCURRENT SESSION CONTROL

Control: The information system limits the number of concurrent sessions for each **non-privileged and privileged** to **maximum of three (3) sessions**.

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 and 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.

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.

Supplemental Guidance: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.

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.

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 by the PSO based on physical accreditation 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/SCTM 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.

Control Enhancements:

(1) SESSION LOCK | PATTERN-HIDING DISPLAYS

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

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: OMB Memorandum 06-16.

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

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:

(1) SESSION TERMINATION | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS

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.

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

[Withdrawn: Incorporated into AC-2 and AU-6].

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

b. Documents and provides supporting rationale in the security plan 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. 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.

Reference AU-3 overprint for guidance on audits for fax machines.

Control Enhancements: None.

(1) PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES
[Withdrawn: Incorporated into AC-14].

References: None.

AC-15 AUTOMATED MARKING

[Withdrawn: Incorporated into MP-3].

References: None.

AC-16 SECURITY ATTRIBUTES

Control: The organization:

a. Provides the means to associate [*Assignment: organization-defined types of security attributes*] having [*Assignment: organization-defined security attribute values*] 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 [Assignment: organization-defined security attributes] for [*Assignment: organization-defined information systems*]; and

d. Determines the permitted [*Assignment: organization-defined values or ranges*] 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.

Organizations can define the types of attributes needed for selected information systems to support missions/business functions. There is potentially a wide range of values that can be assigned to any given security attribute. Release markings could include, for example, US only, NATO, or NOFORN (not releasable to foreign nationals). By specifying permitted attribute ranges and values, organizations can ensure that the security attribute values are meaningful and relevant. The term security labeling refers to the association of security attributes with subjects and objects represented by internal data structures within organizational information systems, to enable information system-based enforcement of information security policies. Security labels include, for example, access authorizations, data life cycle protection (i.e., encryption and data expiration), nationality, affiliation as contractor, and classification of information in accordance with legal and compliance requirements. The term security marking refers to the association of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies. The AC-16 base control represents the requirement for user-based attribute association (marking). The enhancements to AC-16 represent additional requirements including information system-based attribute association (labeling). Types of attributes include, for example, classification level for objects and clearance (access authorization) level for subjects. An example of a value for both of these attribute types is Top Secret. Related controls: AC-3, AC-4, AC-6, AC-21, AU-2, AU-10, SC-16, MP-3.

For example, the organization:

a. Provides the means to associate [**Classification level; accesses; and handling caveat**] having [**Unclassified, Confidential, Secret, Top Secret; Apples, Oranges; HVSACO, FOUO, NOFORN, etc.**] 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 [**Classification level; accesses; and handling caveat**] for [**e.g., Apples Network, FMDR LAN**]; and

d. Determines the permitted [**e.g., user cannot select Apples if user selected Unclassified**] for each of the established security attributes.

For bullets (c) and (d) above, reference DoDM 5200.01 Volume 3, *DoD Information Security Program: Protection of Classified Information*, Enclosure 7, Section 17.

Example implementation for a system where all users are formally accessed to all information: a) attributes (clearance, access, PII, etc.) are identified in the headers/footers, paragraph markings, or in the filename; b) files are saved with these attributes; c) and d) see organization-defined values in example (c and d) above.

Control Enhancements:

(1) SECURITY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION

The information system dynamically associates security attributes with [*Assignment: organization-defined subjects and objects*] in accordance with [*Assignment: organization-defined security policies*] as information is created and combined.

Supplemental Guidance: Dynamic association of security attributes is appropriate whenever the security characteristics of information changes over time. Security attributes may change, for example, due to information aggregation issues (i.e., the security characteristics of individual information elements are different from the combined elements), changes in individual access authorizations (i.e., privileges), and changes in the security category of information. Related control: AC-4.

(2) SECURITY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS

The information system provides authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security attributes.

Supplemental Guidance: The content or assigned values of security attributes can directly affect the ability of individuals to access organizational information. Therefore, it is important for information systems to be able to limit the ability to create or modify security attributes to authorized individuals. Related controls: AC-6, AU-2.

(3) SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM

The information system maintains the association and integrity of [*Assignment: organization-defined security attributes*] to [*Assignment: organization-defined subjects and objects*].

Supplemental Guidance: Maintaining the association and integrity of security attributes to subjects and objects with sufficient assurance helps to ensure that the attribute associations can be used as the basis of automated policy actions. Automated policy actions include, for example, access control decisions or information flow control decisions.

(4) SECURITY ATTRIBUTES | ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS

The information system supports the association of [*Assignment: organization-defined security attributes*] with [*Assignment: organization-defined subjects and objects*] by authorized individuals (or processes acting on behalf of individuals).

Supplemental Guidance: The support provided by information systems can vary to include: (i) prompting users to select specific security attributes to be associated with specific information objects; (ii) employing automated mechanisms for categorizing information with appropriate attributes based on defined policies; or (iii) ensuring that the combination of selected security attributes selected is valid.

Organizations consider the creation, deletion, or modification of security attributes when defining auditable events.

(5) SECURITY ATTRIBUTES | ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES

The information system displays security attributes in human-readable form on each object that the system transmits to output devices to identify [*Assignment: organization-identified special dissemination, handling, or distribution instructions*] using [*Assignment: organization-identified 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.

(6) SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION

The organization allows personnel to associate, and maintain the association of [*Assignment: organization-defined security attributes*] with [*Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-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.

For example, The organization allows the user to select and manage 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.

(7) SECURITY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION

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, cloud-based 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.

(8) SECURITY ATTRIBUTES | ASSOCIATION TECHNIQUES / TECHNOLOGIES

The information system implements [*Assignment: organization-defined techniques or technologies] with [Assignment: organization-defined level of assurance*] in associating security attributes to information.

Supplemental Guidance: The association (i.e., binding) of security attributes to information within information systems is of significant importance with regard to conducting automated access enforcement and flow enforcement actions. The association of such security attributes can be accomplished with technologies/techniques providing different levels of assurance. For example, information systems can cryptographically bind security attributes to information using digital signatures with the supporting cryptographic keys protected by hardware devices (sometimes known as hardware roots of trust).

(9) SECURITY ATTRIBUTES | ATTRIBUTE REASSIGNMENT

The organization ensures that security attributes associated with information are reassigned only via re-grading mechanisms validated using [*Assignment: organization-defined techniques or procedures*].

Supplemental Guidance: Validated re-grading mechanisms are employed by organizations to provide the requisite levels of assurance for security attribute reassignment activities. The validation is facilitated by ensuring that re-grading mechanisms are single purpose and of limited function. Since security attribute reassignments can affect security policy enforcement actions (e.g., access/flow enforcement decisions), using trustworthy re-grading mechanisms is necessary to ensure that such mechanisms perform in a consistent/correct mode of operation.

(10) SECURITY ATTRIBUTES | ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS

The information system provides authorized individuals the capability to define or change the type and value of security attributes available for association with subjects and objects.

Supplemental Guidance: The content or assigned values of security attributes can directly affect the ability of individuals to access organizational information. Therefore, it is important for information systems to be able to limit the ability to create or modify security attributes to authorized individuals only.

References: None.

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, SI-4.

In most cases within the SAP Community, 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.

Control Enhancements:

(1) REMOTE ACCESS | AUTOMATED MONITORING / CONTROL

The information system monitors and controls remote access methods.

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.

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION

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.

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

The information system routes all remote accesses through [*Assignment: organization-defined number*] managed network access control points.

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) REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS

The organization:

a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*Assignment: organization-defined needs*]; and

b. Documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Related control: AC-6.

(5) REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS

[Withdrawn: Incorporated into SI-4].

(6) REMOTE ACCESS | PROTECTION OF INFORMATION

The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

Supplemental Guidance: Related controls: AT-2, AT-3, PS-6.

(7) REMOTE ACCESS | ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS

[Withdrawn: Incorporated into AC-3 (10)].

(8) REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS

[Withdrawn: Incorporated into CM-7].

(9) REMOTE ACCESS | DISCONNECT / DISABLE ACCESS

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within **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.

Termination of the session or connection shall be verified.

References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.

AC-18 WIRELESS ACCESS

Control: The organization:

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

b. Authorizes wireless access to the information system prior to allowing such connections.

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

If no wireless is authorized in the facility, this control still applies. 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 SAP 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 IR and Bluetooth mice). Any exceptions shall be documented and approved by the AO and cognizant PSO [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 will be at the discretion of the AO.

The risks associated with personally-owned wireless technologies used in medical devices must also be assessed. The ISSM/ISSO will work in concert with the PSO/GSSO/CPSO, as appropriate, to allow necessary medical devices to the greatest extent possible, yet within the acceptable risk envelope as determined by the AO in coordination with the Information System Owner. Legal Counsel must be contacted prior to non-approval of any medical device. See organizational/component PED policy for additional detail.

Control Enhancements:

(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION

The information system protects wireless access to the system using authentication of **both users and devices as appropriate; e.g., devices to wireless networks (e.g., Wi-Fi) and users to enterprise services** and encryption.

Supplemental Guidance: Related controls: SC-8, SC-13.

(2) WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS

[Withdrawn: Incorporated into SI-4].

(3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING

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) WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS

The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

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.

(5) WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS

The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

Supplemental Guidance: Actions that may be taken by organizations to limit unauthorized use of wireless communications outside of organization-controlled boundaries include, for example: (i) reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeters of organizations; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) using directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational information systems as well as other systems that may be operating in the area. Related control: PE-19.

References: NIST Special Publications 800-48, 800-94, 800-97.

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.

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

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 PEDs. A PED is any easily transportable, personally-owned or government/contractor-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 (AM)/frequency modulation (FM), satellite), compact discs players, cassette players and recorders, 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]

Policy and procedures related to PEDs are detailed in DoDM 5205.07-V3, Enclosure 3, Section 11, to include a list of authorized PEDs, requirement for PSO and AO (or designee) approval, as required, prior to introduction into a SAPF, and guidance for control of PEDs.

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.

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 PSO assigns responsibilities for the use of these PEDs with SAP information - and establishes procedures to control their use and accountability to ensure SAP information is protected from unauthorized disclosure.

Control Enhancements:

(1) ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE / PORTABLE STORAGE DEVICES

[Withdrawn: Incorporated into MP-7].

(2) ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES

[Withdrawn: Incorporated into MP-7].

(3) ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER

[Withdrawn: Incorporated into MP-7].

(4) ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION

The organization:

(a) Prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and

(b) Enforces the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information:

(1) Connection of unclassified mobile devices to classified information systems is prohibited;

(2) Connection of unclassified mobile devices to unclassified information systems requires approval from the authorizing official;

(3) Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and

(4) Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by **ISSM / PSO**, and if classified information is found, the incident handling policy is followed.

(c) Restricts the connection of classified mobile devices to classified information systems in accordance with [*Assignment: organization-defined security policies*].

Supplemental Guidance: Related controls: CA-6, IR-4.

(5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION

The organization employs [*Selection: full-device encryption; container encryption*] to protect the confidentiality and integrity of information on **all mobile devices**.

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.

PEDs that contain classified or controlled unclassified information (CUI) information must be encrypted with a National Security Agency (NSA) or DoD-approved encryption standard.

References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.

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.

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, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems.

For some external information systems (i.e., information systems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

This control does not apply to the use of external information systems to access public interfaces to organizational information systems (e.g., individuals accessing federal information through www.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.

An external information system may be a standalone or an interconnected system/service. Providers of external information systems should provide the PSO/ISSM with an external information system memorandum of understanding (MOU) (e.g., no exchange of resources), or memorandum of agreement (e.g., exchange of resources such as personnel, services, funds), as well as SOP and ATO or approval letter. An external information system MOU/MOA includes information such as the ATO date if applicable, technical concerns (e.g., wireless (Bluetooth, etc.), cameras are turned off, microphones are disabled), resources required (e.g., personnel), and additional system information as required (e.g., classified vs. corporate system). Ensure a co-utilization agreement (CUA) is in place for the facility, if applicable.

In those cases where the external system connects to the SAP system, ensure 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 or MOA. [AC-20(1)(a)]

For SAP Support Systems (e.g., card readers, alarm systems) reference PE-2 guidance.

Prior to allowing corporate unclassified systems in the SAPF, the CPSO and ISSM/ISSO in coordination with corporate IT ensures endpoint security is appropriately hardened/configured, e.g., wireless and microphones are disabled prior to the PSO approving entry to the SAPF.

Control Enhancements:

(1) USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

(a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

(b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

Supplemental Guidance: This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations. Related control: CA-2.

(2) USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES

The organization [*Selection: restricts; prohibits*] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

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.

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

The organization [*Selection: restricts; prohibits*] the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.

Supplemental Guidance: Non-organizationally owned devices include devices owned by other organizations (e.g., federal/state agencies, contractors) 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, for example: (i) requiring the implementation of organization-approved security controls prior to authorizing such connections; (ii) limiting access to certain types of information, services, or applications; (iii) using virtualization techniques to limit processing and storage activities to servers or other system components provisioned by the organization; and (iv) 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) USE OF EXTERNAL INFORMATION SYSTEMS | NETWORK ACCESSIBLE STORAGE DEVICES

The organization prohibits the use of [*Assignment: organization-defined network accessible storage devices*] in external information systems.

Supplemental Guidance: Network accessible storage devices in external information systems include, for example, online storage devices in public, hybrid, or community cloud-based systems.

References: FIPS Publication 199.

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 for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and

b. Employs [*Assignment: organization-defined automated mechanisms or manual processes*] 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., VTCs, phone conversations, and fax transmittals. The organization will use a PSO-approved mechanism to ensure informed security decisions are made, preventing inadvertent disclosures. For example, the organization provides either a tool (e.g., Access Look-up, Joint Access Database Environment (JADE)) or appropriate guidance on a manual process (e.g., contact PSO, HR) to assist the user in making an informed decision prior to sharing information.

Control Enhancements:

(1) INFORMATION SHARING | AUTOMATED DECISION SUPPORT

The information system enforces information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.

(2) INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL

The information system implements information search and retrieval services that enforce [*Assignment: organization-defined information sharing restrictions*].

References: None.

AC-22 PUBLICLY ACCESSIBLE CONTENT

Control: The organization:

a. Designates individuals authorized to post information onto a publicly accessible information system;

b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

d. Reviews the content on the publicly accessible information system for nonpublic information **at least quarterly or as new information is posted** and removes such information, if discovered.

Supplemental Guidance: In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by organizational policy. Related controls: AC-3, AC-4, AT-2, AT-3, AU-13.

> From an organizational perspective this is a common control. Typically, this control is addressed by a Public Affairs Office or similar entity.
>
> Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information, as is classified information. The information to be posted must be reviewed by the appropriate organizational element (e.g., Special Security Office (SSO), Foreign Disclosure Office (FDO), Legal, Public Affairs) prior to being posted on the organization’s information system**.** [AC-22.c] [AC-22.d] Unauthorized information, if discovered, shall be removed immediately from the publicly accessible information system and reported to the PSO and information owner. Reference IR-6.

Control Enhancements: None.

References: None.

AC-23 DATA MINING PROTECTION

Control: The organization employs [*Assignment: organization-defined data mining prevention and detection techniques*] for [*Assignment: organization-defined data storage objects*] to adequately detect and protect against data mining.

Supplemental Guidance: Data storage objects include, for example, databases, database records, and database fields. 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. 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.

AC-24 ACCESS CONTROL DECISIONS

Control: The organization establishes procedures to ensure [*Assignment: organization-defined access control decisions*] are applied to each access request prior to access enforcement.

Supplemental Guidance: Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when information systems enforce access control decisions. While it is very common to have access control decisions and access enforcement implemented by the same entity, it is not required and it is not always an optimal implementation choice. For some architectures and distributed information systems, different entities may perform access control decisions and access enforcement.

Control Enhancements:

(1) ACCESS CONTROL DECISIONS | TRANSMIT ACCESS AUTHORIZATION INFORMATION

The information system transmits [*Assignment: organization-defined access authorization information*] using [*Assignment: organization-defined security safeguards*] to [*Assignment: organization-defined information systems*] that enforce access control decisions.

Supplemental Guidance: In distributed information systems, authorization processes and access control decisions may occur in separate parts of the systems. In such instances, authorization information is transmitted securely so timely access control decisions can be enforced at the appropriate locations. To support the access control decisions, it may be necessary to transmit as part of the access authorization information, supporting security attributes. This is due to the fact that in distributed information systems, there are various access control decisions that need to be made and different entities (e.g., services) make these decisions in a serial fashion, each requiring some security attributes to make the decisions. Protecting access authorization information (i.e., access control decisions) ensures that such information cannot be altered, spoofed, or otherwise compromised during transmission.

(2) ACCESS CONTROL DECISIONS | NO USER OR PROCESS IDENTITY

The information system enforces access control decisions based on [*Assignment: organization-defined security attributes*] that do not include the identity of the user or process acting on behalf of the user.

Supplemental Guidance: In certain situations, it is important that access control decisions can be made without information regarding the identity of the users issuing the requests. These are generally instances where preserving individual privacy is of paramount importance. In other situations, user identification information is simply not needed for access control decisions and, especially in the case of distributed information systems, transmitting such information with the needed degree of assurance may be very expensive or difficult to accomplish.

References: None.

AC-25 REFERENCE MONITOR

Control: The information system implements a reference monitor for [*Assignment: organization-defined access control policies*] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.

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. Reference monitors typically enforce mandatory access control policies—a type of access control that restricts access to objects based on the identity of subjects or groups to which the subjects belong. The access controls are mandatory because subjects with certain privileges (i.e., access permissions) are restricted from passing those privileges on to any other subjects, either directly or indirectly—that is, the information system strictly enforces the access control policy based on the rule set established by the policy. The tamperproof property of the reference monitor prevents adversaries from compromising the functioning of the mechanism. The always invoked property prevents adversaries from bypassing the mechanism and hence violating the security policy. The smallness property helps to ensure the completeness in the analysis and testing of the mechanism to detect weaknesses or deficiencies (i.e., latent flaws) that would prevent the enforcement of the security policy. Related controls: AC-3, AC-16, SC-3, SC-39.

Control Enhancements: None.

References: None.

FAMILY: AWARENESS AND TRAINING

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]

   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 **at least 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.

DoD SAP-specific policy and procedures related to security awareness and training are defined in the remainder of this section.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-16, 800-50, 800-100.

AT-2 SECURITY AWARENESS TRAINING

Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;

b. When required by information system changes; and

c. **At least annually** thereafter.

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. Security awareness training will be conducted:

- During in-processing. Site specific information will be briefed based on the mission and requirements of the job.

- Upon receipt of a USERID and authenticator. The Privileged User, ISSO or their alternate will brief the user on his/her IA responsibilities.
- 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.
- Periodically, refresher training and awareness may also be delivered through staff meetings, online delivery systems, or similar venues.
- To include lessons learned captured from incident handling and response. See [IR-4].

Control Enhancements:

(1) SECURITY AWARENESS | PRACTICAL EXERCISES

The organization includes practical exercises in security awareness training that simulate actual cyber attacks.

Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Related controls: CA-2, CA-7, CP-4, IR-3.

(2) SECURITY AWARENESS | INSIDER THREAT

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

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.

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.

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. Role-based security training also applies to contractors providing services to federal agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.

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.

General User Training
General user training will include, but is not limited to, the following:

- 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.
- The organization’s policy regarding appropriate use of IS resources as specified in the User Agreement and the possible repercussions of misuse or abuse.
- How to protect the physical area, media, and equipment (e.g., door access, alarms, care of hard drives, CDs).
- How to protect authenticators and operate the applicable system security features (e.g., setting access control rights to files created by the user).
- How to recognize and report suspected security violations and incidents.
- Understanding the importance of classification and control marking compliance.
- 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:

- Completion of General user training.
- Rules of behavior, as they apply to the privileged user.
- 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.
- The organization’s policy regarding appropriate privileged use of IS resources and the possible repercussions of misuse or abuse.
- How to protect the system (e.g., maintenance and backup, care of system media, protection and retention of audit logs, endpoint security).
- How to protect passwords, or other authentication devices/mechanisms, and be familiar with operating system security features and technical safeguards of the system.
- How to recognize and report potential security vulnerabilities, threats, security violations, or incidents.
- Technical actions to take in the event of a data spill. Reference [IR-2].
- How to implement and use specific IA products provided by the organization.
- IA training and certification in compliance with DoD 8570.01-M, or its replacement manual based on DoDD 8140.01, as required for designated positions.

Prior to obtaining privileged user system access credentials:

- Complete the applicable Privileged User Access Training as required by agency/service element. See also Security Training [AT-3].
- Read and sign the applicable Service/Agency privileged user agreement for SAP information systems. The privileged user agreement must include the language in Attachment 2 the "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," in accordance with DoDI 8500.01, Cybersecurity, which is posted as stated in DoDI 8500.01 on the IASE Website (http://iase.disa.mil). Where a user will obtain both a general user account and a privileged user account, two separate user agreements should be used.
- Provide the training completion certificate and privileged user agreement to the ISSM.

Assured File Transfer (AFT) Training

Also reference [AC-4]

An individual performing data transfers between systems of differing security domains is commonly referred to as a DTA. The DTA is performing a security-relevant function in providing endpoint security during a data transfer and is therefore, by definition, a privileged user. However, the DTA role is not specifically called out in 8570.01-M and therefore does not required an '8570' certification unless the AO directs otherwise.

DTAs must be identified in writing. AFT training for DTAs will include, but is not limited to the following:

- Training in the use of data review and sanitization tools (automated and manual).
- Working knowledge of the Program Security Guide and Classification Marking Guide.
- File formats permissible for trusted downloading.
- Authorized media formats and marking requirements.
- Program management approval and Security process compliance review.

Control Enhancements:

(1) SECURITY TRAINING | ENVIRONMENTAL CONTROLS

The organization provides [*Assignment: organization-defined personnel or roles*] with initial and a**t least annually or when sufficient changes are made to environmental control systems** training in the employment and operation of environmental controls.

Supplemental Guidance: Environmental controls include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility. Organizations identify personnel with specific roles and responsibilities associated with environmental controls requiring specialized training. Related controls: PE-1, PE-13, PE-14, PE-15.

(2) SECURITY TRAINING | PHYSICAL SECURITY CONTROLS

The organization provides [*Assignment: : organization-defined personnel or roles*] with initial and **at least annually or when sufficient changes are made to physical security systems** training in the employment and operation of physical security controls.

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.

(3) SECURITY TRAINING | PRACTICAL EXERCISES

The organization includes practical exercises in security training that reinforce training objectives.

Supplemental Guidance: Practical exercises may include, for example, security training for software developers that includes simulated cyber attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

(4) SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

The organization provides training to its personnel on [*Assignment: organization-defined indicators of malicious code*] to recognize suspicious communications and anomalous behavior in organizational information systems.

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 (e.g., receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender but who appears to be from a known sponsor or contractor). 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.

References: C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); NIST Special Publications 800-16, 800-50.

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 (5) years**.

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.

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

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

Initial training records must contain legal signatures, or FIPS 140-2-compliant digital signatures, of users who received the training. 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 professional certifications and training records in compliance with DoD 8570.01-M or its follow-on.

Control Enhancements: None.

References: None.

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

[Withdrawn: Incorporated into PM-15].

FAMILY: AUDIT AND ACCOUNTABILITY

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

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.

DoD SAP-specific policy and procedures related to audit and accountability are defined in the remainder of this section.

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:

- Detecting unauthorized access to information
- Establishing a culture of responsibility and accountability
- Reducing the risk associated with inappropriate accesses (behavior may be altered when individuals know they are being monitored)
- 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
- Tracking disclosures of sensitive and/or classified information
- Responding to concerns regarding unauthorized access
- 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)
- Detecting new threats and intrusion attempts
- Identifying potential problems
- 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:

- **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.
- **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.
- **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.
- **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, 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 approval to operate must specify approval to implement manual audits.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

AU-2 AUDIT EVENTS

Control: The organization:

a. Determines that the information system is capable of auditing the following events:

1. Authentication events:

(1) Logons (Success/Failure)

(2) Logoffs (Success)

2. Security Relevant File and Objects events:

(1) Create (Success/Failure)

(2) Access (Success/Failure)

(3) Delete (Success/Failure)

(4) Modify (Success/Failure)

(5) Permission Modification (Success/Failure)

(6) Ownership Modification (Success/Failure)

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

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

5. User and Group Management events:

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

(2) Group/Role add, delete, modify (Success/Failure)

6. Use of Privileged/Special Rights events:

(1) Security or audit policy changes (Success/Failure)

(2) Configuration changes (Success/Failure)

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

8. Privilege/Role escalation (Success/Failure)

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

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

11. Print to a device (Success/Failure)

12. Print to a file (e.g., pdf format) (Success/Failure)

13. Application (e.g., Adobe, Firefox, MS Office Suite) initialization (Success/Failure);

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Determines that the following events are to be audited within the information system: **same as 'a' above, during all periods of system operation**.

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, 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.

Be aware that [AU-2.a] bullet 13, Application, may generate more audits than deemed necessary. Tailoring audit collection requirements related to specific applications is recommended.

Control Enhancements:

(1) AUDIT EVENTS | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES

[Withdrawn: Incorporated into AU-12].

(2) AUDIT EVENTS | SELECTION OF AUDIT EVENTS BY COMPONENT

[Withdrawn: Incorporated into AU-12].

(3) AUDIT EVENTS | REVIEWS AND UPDATES

The organization reviews and updates the audited events **at least annually**.

Supplemental Guidance: Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

The review shall include coordination with other organizational entities requiring audit-related information (e.g., Incident Response, Counterintelligence) to enhance mutual support and to help guide the selection of auditable events.

(4) AUDIT EVENTS | PRIVILEGED FUNCTIONS

[Withdrawn: Incorporated into AC-6 (9)].

References: NIST Special Publication 800-92; Web: http://idmanagement.gov.

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.

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.

Specifically, audit records shall contain, at a minimum, the following content:

- USERID
- Type of event/action
- Success or failure of event/action
- Date
- Time
- Terminal or workstation ID
- Entity that initiated event/action
- Entity that completed event/action
- Remote Access

If manual audit collection is approved by the AO, the audit records shall contain, at a minimum, the following content:

- Date
- Identification of the user
- Time the user logs on and off the system
- Function(s) performed
- 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)). Reference DoDM 5205.07-V1, Enclosure 5, para 2.b. These logs will be maintained for one year and must include the following information:

- Sender's name, organization and telephone number
- Date and time of fax transmission
- Classification level of the information
- Recipient's name, organization and telephone number

Control Enhancements:

(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

The information system generates audit records containing the following additional information: [*Assignment: organization-defined additional, more detailed information*].

Supplemental Guidance: Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.

(2) CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT

The information system provides centralized management and configuration of the content to be captured in audit records generated by [*Assignment: organization-defined information system components*].

Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Related controls: AU-6, AU-7.

References: None.

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates audit record storage capacity in accordance with **community best practice and configures auditing to reduce the likelihood of such capacity being exceeded**.

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.

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).

Control Enhancements:

(1) AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE

The information system off-loads audit records [*Assignment: organization-defined frequency]* onto a different system or media than the system being audited.

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.

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

References: None.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts [[*Assignment: organization-defined personnel or roles*]] in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

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

Control Enhancements:

(1) RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY

The information system provides a warning to [*Assignment: organization-defined personnel, roles, and/or locations*] within [*Assignment: organization-defined time period*] when allocated audit record storage volume reaches **maximum of 75 percent maximum audit record storage capacity** of repository maximum audit record storage capacity.

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

(2) RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS

The information system provides an alert in [*Assignment: organization-defined real-time period*] to [*Assignment: organization-defined personnel, roles, and/or locations*] when the following audit failure events occur: **minimally but not limited to: auditing software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded**.

Supplemental Guidance: Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

(3) RESPONSE TO AUDIT PROCESSING FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS

The information system enforces configurable network communications traffic volume thresholds reflecting limits on auditing capacity and [*Selection: rejects; delays*] network traffic above those thresholds.

Supplemental Guidance: Organizations have the capability to reject or delay the processing of network communications traffic if auditing such traffic is determined to exceed the storage capacity of the information system audit function. The rejection or delay response is triggered by the established organizational traffic volume thresholds which can be adjusted based on changes to audit storage capacity.

(4) RESPONSE TO AUDIT PROCESSING FAILURES | SHUTDOWN ON FAILURE

The information system invokes a [*Selection: full system shutdown; partial system shutdown; degraded operational mode with limited mission/business functionality available*] in the event of [*Assignment: organization-defined audit failures*], unless an alternate audit capability exists.

Supplemental Guidance: Organizations determine the types of audit failures that can trigger automatic information system shutdowns or degraded operations. Because of the importance of ensuring mission/business continuity, organizations may determine that the nature of the audit failure is not so severe that it warrants a complete shutdown of the information system supporting the core organizational missions/business operations. In those instances, partial information system shutdowns or operating in a degraded mode with reduced capability may be viable alternatives. Related control: AU-15.

References: None.

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 findings to [*Assignment: organization-defined personnel or roles*].

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 VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority. 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, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.

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/or PSO.

Control Enhancements:

(1) AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION

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.

(2) AUDIT REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS

[Withdrawn: Incorporated into SI-4].

(3) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES

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) AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS

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.

(5) AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES

The organization integrates analysis of audit records with analysis of [*Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; [Assignment: organization-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.

(6) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING

The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Supplemental Guidance: The correlation of physical audit information and audit logs from information systems may assist organizations in identifying examples of suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identity for logical access to certain information systems with the additional physical security information that the individual was actually present at the facility when the logical access occurred, may prove to be useful in investigations.

(7) AUDIT REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS

The organization specifies the permitted actions for each [Selection (one or more): information system process; role; user] associated with the review, analysis, and reporting of audit information.

Supplemental Guidance: Organizations specify permitted actions for information system processes, roles, and/or users associated with the review, analysis, and reporting of audit records through account management techniques. Specifying permitted actions on audit information is a way to enforce the principle of least privilege. Permitted actions are enforced by the information system and include, for example, read, write, execute, append, and delete.

(8) AUDIT REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS

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.

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

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.

(10) AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT

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.

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:

(1) AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING

The information system provides the capability to process audit records for events of interest based on [*Assignment: organization-defined audit fields within audit records*].

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, 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.

(2) AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH

The information system provides the capability to sort and search audit records for events of interest based on the content of [*Assignment: organization-defined audit fields within audit records*].

Supplemental Guidance: Sorting and searching of audit records may be based upon the contents of audit record fields, for example: (i) date/time of events; (ii) user identifiers; (iii) Internet Protocol (IP) addresses involved in the event; (iv) type of event; or (v) event success/failure.

References: None.

AU-8 TIME STAMPS

Control: The information system:

a. Uses internal system clocks to generate time stamps for audit records; and

b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets **organization-defined granularity of time measurement of a minimum of one (1) minute.**

Supplemental Guidance: Time stamps generated by the information system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. Related controls: AU-3, AU-12.

Control Enhancements:

(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

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**.

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

(2) TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE

The information system identifies a secondary authoritative time source that is located in a different geographic region than the primary authoritative time source.

> For example, every 24 hours verify internal information system clocks are in sync against an internal source, e.g., domain controller, NTP server. Then, once a month sync up the source clock (e.g., domain controller) with an external source, e.g., USNO.

References: None.

AU-9 PROTECTION OF AUDIT INFORMATION

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

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.

> 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.

Control Enhancements:

(1) PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE MEDIA

The information system writes audit trails to hardware-enforced, write-once media.

Supplemental Guidance: This control enhancement applies to the initial generation of audit trails (i.e., the collection of audit records that represents the audit information to be used for detection, analysis, and reporting purposes) and to the backup of those audit trails. The enhancement does not apply to the initial generation of audit records prior to being written to an audit trail. Write-once, read-many (WORM) media includes, for example, Compact Disk-Recordable (CD-R) and Digital Video Disk-Recordable (DVD-R). In contrast, the use of switchable write-protection media such as on tape cartridges or Universal Serial Bus (USB) drives results in write-protected, but not write-once, media. Related controls: AU-4, AU-5.

(2) PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS

The information system backs up audit records **at least weekly** onto a physically different system or system component than the system or component being audited.

Supplemental Guidance: This control enhancement helps to ensure that a compromise of the information system being audited does not also result in a compromise of the audit records. Related controls: AU-4, AU-5, AU-11.

(3) PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION

The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

Supplemental Guidance: Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash. Related controls: AU-10, SC-12, SC-13.

(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

The organization authorizes access to management of audit functionality to only [*Assignment: organization-defined subset of privileged users Assignment: organization-defined subset of privileged users*].

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.

> 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.
>
> The AO may tailor in AU-9(6) to allow read only for a system administrator requiring access to audits for troubleshooting/diagnostics purposes.

(5) PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION

The organization enforces dual authorization for [*Selection (one or more): movement; deletion*] of **any security related audit information**.

Supplemental Guidance: Organizations may choose different selection options for different types of audit information. Dual authorization mechanisms require the approval of two authorized individuals in order to execute. Dual authorization may also be known as two-person control. Related controls: AC-3, MP-2.

(6) PROTECTION OF AUDIT INFORMATION | READ ONLY ACCESS

The organization authorizes read-only access to audit information to [*Assignment: organization-defined subset of privileged users*.

Supplemental Guidance: Restricting privileged user authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users (e.g., deleting audit records to cover up malicious activity).

References: None.

AU-10 NON-REPUDIATION

Control: The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [*Assignment: organization-defined actions to be covered by non-repudiation*].

Supplemental Guidance: Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts). Related controls: SC-12, SC-8, SC-13, SC-16, SC-17, SC-23.

Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts). Digital signatures, if implemented, shall employ Federal Information Processing Standards (FIPS)-validated or National Security Agency (NSA)-approved cryptography, as appropriate for the classification of the information system. Tactical/deployable information systems may be developed without all the features and security controls of standard information systems. Non-repudiation requirements for these systems should be reviewed for mission impact.

Control Enhancements:

(1) NON-REPUDIATION | ASSOCIATION OF IDENTITIES

The information system:

(a) Binds the identity of the information producer with the information to [*Assignment: organization-defined strength of binding*]; and

(b) Provides the means for authorized individuals to determine the identity of the producer of the information.

Supplemental Guidance: This control enhancement supports audit requirements that provide organizational personnel with the means to identify who produced specific information in the event of an information transfer. Organizations determine and approve the strength of the binding between the information producer and the information based on the security category of the information and relevant risk factors. Related controls: AC-4, AC-16.

(2) NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY

The information system:

(a) Validates the binding of the information producer identity to the information at [*Assignment: organization-defined frequency*]; and

(b) Performs [*Assignment: organization-defined actions*] in the event of a validation error.

Supplemental Guidance: This control enhancement prevents the modification of information between production and review. The validation of bindings can be achieved, for example, by the use of cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically. Related controls: AC-3, AC-4, AC-16.

(3) NON-REPUDIATION | CHAIN OF CUSTODY

The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.

Supplemental Guidance: Chain of custody is a process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each person who handled the evidence, the date and time it was collected or transferred, and the purpose for the transfer. If the reviewer is a human or if the review function is automated but separate from the release/transfer function, the information system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, this control enhancement provides organizational officials the means to identify who reviewed and released the information. In the case of automated reviews, this control enhancement ensures that only approved review functions are employed. Related controls: AC-4, AC-16.

(4) NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY

The information system:

(a) Validates the binding of the information reviewer identity to the information at the transfer or release points prior to release/transfer between [*Assignment: organization-defined security domains*]; and

(b) Performs [*Assignment: organization-defined actions*] in the event of a validation error.

Supplemental Guidance: This control enhancement prevents the modification of information between review and transfer/release. The validation of bindings can be achieved, for example, by the use of cryptographic checksums. Organizations determine validations are in response to user requests or generated automatically. Related controls: AC-4, AC-16.

(5) NON-REPUDIATION | DIGITAL SIGNATURES

[Withdrawn: Incorporated into SI-7].

References: None.

AU-11 AUDIT RECORD RETENTION

Control: The organization retains audit records for **a minimum of 5 years for SAP data, Sensitive Compartmented Information and Sources And Methods Intelligence information AND A minimum of 1 year for all other information (Unclassified through Collateral Top Secret)** to provide support for 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 (IG) are within the one (1) year mark, audit records going back five (5) years provide historic information that is frequently used in espionage cases for damage assessment purposes to determine what the (alleged) perpetrator may have accessed.
>
> The AO has the authority to scale back the number of years retained depending upon the mission supported by the system, e.g., a short-lived research and development (R&D) or science and technology (S&T) effort, tactical or fleet capability, platform IT (PIT) designation.

Control Enhancements:

(1) AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY

The organization employs **a 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.

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 [*Assignment: organization-defined personnel or roles*] 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:

(1) AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL

The information system compiles audit records from [*Assignment: organization-defined information system components*] into a system-wide (logical or physical) audit trail that is time-correlated to within **the tolerance defined in AU-8**.

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.

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.

(2) AUDIT GENERATION | STANDARDIZED FORMATS

The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

Supplemental Guidance: Audit information that is normalized to common standards promotes interoperability and exchange of such information between dissimilar devices and information systems. This facilitates production of event information that can be more readily analyzed and correlated. Standard formats for audit records include, for example, system log records and audit records compliant with Common Event Expressions (CEE). If logging mechanisms within information systems do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.

(3) AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS

The information system provides the capability for [*Assignment: organization-defined individuals or roles*] to change the auditing to be performed on [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds*].

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.

AU-13 MONITORING FOR INFORMATION DISCLOSURE

Control: The organization monitors [*Assignment: organization-defined open source information and/or information sites*] [*Assignment: organization-defined frequency*] for evidence of unauthorized disclosure of organizational information.

Supplemental Guidance: Open source information includes, for example, social networking sites. Related controls: PE-3, SC-7.

Control Enhancements:

(1) MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS

The organization employs automated mechanisms to determine if organizational information has been disclosed in an unauthorized manner.

Supplemental Guidance: Automated mechanisms can include, for example, automated scripts to monitor new posts on selected websites, and commercial services providing notifications and alerts to organizations.

(2) MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES

The organization reviews the open source information sites being monitored [*Assignment: organization-defined frequency*].

References: None.

AU-14 SESSION AUDIT

Control: The information system provides the capability for authorized users to select a user session to capture/record or view/hear.

Supplemental Guidance: Session audits include, for example, monitoring keystrokes, tracking websites visited, and recording information and/or file transfers. Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, or standards. Related controls: AC-3, AU-4, AU-5, AU-9, AU-11.

Verify system is capable of performing session audits, but do not initiate without legal counsel and AO involvement. This control may be used to audit file transfers of DTAs.

Control Enhancements:

(1) SESSION AUDIT | SYSTEM START-UP

The information system initiates session audits at system start-up.

(2) SESSION AUDIT | CAPTURE/RECORD AND LOG CONTENT

The information system provides the capability for authorized users to capture/record and log content related to a user session.

(3) SESSION AUDIT | REMOTE VIEWING / LISTENING

The information system provides the capability for authorized users to remotely view/hear all content related to an established user session in real time.

References: None.

AU-15 ALTERNATE AUDIT CAPABILITY

Control: The organization provides an alternate audit capability in the event of a failure in primary audit capability that provides [*Assignment: organization-defined alternate audit functionality*].

Supplemental Guidance: Since an alternate audit capability may be a short-term protection employed until the failure in the primary auditing capability is corrected, organizations may determine that the alternate audit capability need only provide a subset of the primary audit functionality that is impacted by the failure. Related control: AU-5.

Control Enhancements: None.

References: None.

AU-16 CROSS-ORGANIZATIONAL AUDITING

Control: The organization employs [*Assignment: organization-defined methods*] for coordinating [*Assignment: organization-defined audit information*] among external organizations when audit information is transmitted across organizational boundaries.

Supplemental Guidance: When organizations use information systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals that requested particular services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance ramifications. Therefore, it is often the case that cross-organizational auditing (e.g., the type of auditing capability provided by service-oriented architectures) simply captures the identity of individuals issuing requests at the initial information system, and subsequent systems record that the requests emanated from authorized individuals. Related control: AU-6.

This control may be met through use of an ISA, SLA, or MOA.

Control Enhancements:

(1) CROSS-ORGANIZATIONAL AUDITING | IDENTITY PRESERVATION

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.

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

The organization provides cross-organizational audit information to [*Assignment: organization-defined organizations*] based on [*Assignment: organization-defined cross-organizational sharing agreements*].

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.

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and

b. Reviews and updates the current:

1. Security assessment and authorization policy **at least 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.

DoD SAP-specific policy and procedures related to security assessment and authorization are defined in the remainder of this section.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100.

CA-2 SECURITY ASSESSMENTS

Control: The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:

1. Security controls and control enhancements under assessment;

2. Assessment procedures to be used to determine security control effectiveness; and

3. Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system and its environment of operation **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 **SCA at a minimum**.

Supplemental Guidance: Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.

The initial security assessment, frequently conducted by the SCA, or other AO designee, 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. The AO determines the level of assessor impartiality required, based on the criticality and sensitivity of the information system, to ensure the assessment results produced are sound and can be used to make a credible, risk-based decision.

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. Security assessments are routinely conducted by SCAs, ISOs, common control providers, ISSM/ISSOs, independent assessors, auditors, and IGs during the system life cycle to ensure that security controls are effective and continue to be effective in the operational environment where the system is deployed. After the initial authorization, the organization continues to assess the security controls on an ongoing basis. The assessments are based on the continuous monitoring plan developed by the ISO or CCP and approved by the AO. Types of assessments include self-assessments as well as independent assessments.

As part of the security assessment process, a Security Assessment Plan must be developed either by the ISO, ISSM/ISSO, ISSE or the SCA. The Security Assessment Plan provides the objectives for the security assessment, the proposed method for verifying compliance with security controls, a proposed schedule for conducting the assessment, and assessment procedures. For the DoD SAP Community and for all IS under the purview of the SAP AO, the Security Assessment Plan is embodied in the information provided in the SSP, the SCTM, and the Security Control Assessment Procedures, all of which must be reviewed and approved by the SCA.

The following steps will be considered when developing the Security Assessment Plan:

- Determine which security controls/control enhancements are to be included in the assessment based upon the contents of the SSP and the purpose/scope of the assessment and whether this is a complete or partial assessment.
- Select the appropriate assessment procedures to be used during the assessment based on the security controls and control enhancements that are to be included in the assessment. Refer to NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans,* Appendix F, for an assessment procedure for each security control and control enhancement.
- Tailor the selected assessment procedures to meet organizational needs (e.g., select appropriate assessment methods and objectives).
- Develop additional assessment procedures to address any security requirements or controls that are not sufficiently covered by NIST SP 800-53A.
    - The ISO may develop and implement additional security controls, and therefore assessments, specific to the organization based on organizational policies, mission or business function requirements, and the risk assessment. See the Risk Assessment section for further details regarding assessment of risk. The assessment procedures developed are subsequently integrated into the Security Assessment Plan.
- Optimize the assessment procedures to reduce duplication of effort (e.g., sequencing and consolidating assessment procedures) to provide cost-effective assessment solutions.
    - The assessment of some security controls before others may provide information that facilitates understanding and assessment of other controls.

At the conclusion of the security assessment activity with a goal of receiving authorization or reauthorization to operate, a SAR shall be produced by the individual conducting the assessment, e.g., SCA. The SAR conveys the results of the security assessment to appropriate organizational officials. The SAR is included in the security authorization package that is reviewed by the SCA and provided to the AO with the information necessary to make a credible, risk-based decision on whether to place an information system into operation or continue its operation. The SAR details any shortcomings and/or vulnerabilities identified during the security assessment and a POA&M addressing the fixes, workarounds, etc. is developed.

Security assessment activities and a resulting SAR are also conducted/produced by the ISO/ISSM/ISSO as part of continuous monitoring and other activities as outlined in the NIST Supplemental Guidance for this control.

Information revealing specific vulnerabilities (other than the known vulnerabilities of widely available commercial products) and the compiled results of vulnerability analyses for all SAP systems shall be classified in accordance with the Program Security Classification Guide (SCG), usually at a minimum level of SECRET, and requires appropriate protection levels to control access to the information. When appropriate, the information will be marked Handle via Special Access Channels Only (HVSACO) to ensure a review by the Initial Denial Authority is required before the information is considered for release outside of SAP control channels.

The information detailed in the SAR and POA&M (reference CA-5) is used by the AO when making the approval decision.

Control Enhancements:

(1) SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS

The organization employs assessors or assessment teams with **AO determined level of impartiality based on the risk assessment for the system** to conduct security control assessments.

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.

(2) SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS

The organization includes as part of security control assessments, [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]*].

Supplemental Guidance: Organizations can employ information system monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security. Organizations conduct assessment activities in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes. Related controls: PE-3, SI-2.

(3) SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS

The organization accepts the results of an assessment of [*Assignment: organization-defined information system*] performed by [*Assignment: organization-defined external organization*] when the assessment meets [*Assignment: organization-defined requirements*].

Supplemental Guidance: Organizations may often rely on assessments of specific information systems by other (external) organizations. Utilizing such existing assessments (i.e., reusing existing assessment evidence) can significantly decrease the time and resources required for organizational assessments by limiting the amount of independent assessment activities that organizations need to perform. The factors that organizations may consider in determining whether to accept assessment results from external organizations can vary. Determinations for accepting assessment results can be based on, for example, past assessment experiences one organization has had with another organization, the reputation that organizations have with regard to assessments, the level of detail of supporting assessment documentation provided, or mandates imposed upon organizations by federal legislation, policies, or directives.

References: Executive Order 13587; FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137.

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 Interconnection Security Agreements **at least annually**.

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 and 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.

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 (CDSE), e.g., CA SAPCO, AO. All cross domain connections shall comply with the security controls identified by the UCDSMO.

The direct connection of any information system to an external network is prohibited. No 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.

Control Enhancements:

(1) SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

The organization prohibits the direct connection of an **all unclassified NSS** to an external network without the use of [*Assignment: organization-defined boundary protection device*].

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 unclassified national security systems and external networks. This control enhancement is required for organizations processing, storing, or transmitting Controlled Unclassified Information (CUI).

(2) SYSTEM INTERCONNECTIONS | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

The organization prohibits the direct connection of a classified, national security system to an external network without the use of [*Assignment: organization-defined boundary protection device*].

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.

(3) SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS

The organization prohibits the direct connection of an [*Assignment: organization-defined unclassified, non-national security system]* to an external network without the use of [*Assignment; organization-defined boundary protection device].*

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 unclassified non-national security systems and external networks. This control enhancement is required for organizations processing, storing, or transmitting Controlled Unclassified Information (CUI).

(4) SYSTEM INTERCONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS

The organization prohibits the direct connection of an [*Assignment: organization-defined information system*] to a public network.

Supplemental Guidance: A public network is any network accessible to the general public including, for example, the Internet and organizational extranets with public access.

(5) SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS

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.

CA-4 SECURITY CERTIFICATION

[Withdrawn: Incorporated into CA-2].

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 findings from security controls assessments, security impact analyses, and continuous monitoring activities.

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.

POA&Ms are the authoritative management tool used by the organization (including the AO, SCA, PSO) 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 findings and recommendations from the SAR, or as a minimum, providing that information via the SAR to the ISO.
The ISO shall describe the planned tasks for correcting weaknesses and addressing any residual findings. The POA&M shall identify:

- Tasks to be accomplished with a recommendation for completion either before or after information system implementation.
- Resources required to accomplish the tasks.
- Any milestones in meeting the tasks, to include percentage completed.
- Scheduled completion dates for the milestones.
- Status of tasks (completed, ongoing, delayed, planned)

The POA&M is used by the AO and SCA to monitor the progress in mitigating any findings. 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. Once an authorization is issued with a POA&M, adjusting the approved milestones and scheduled completion dates is not allowed without coordination with AO.

Control Enhancements:

(1) PLAN OF ACTION AND MILESTONES | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY
The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.

References: OMB Memorandum 02-01; NIST Special Publication 800-37.

CA-6 SECURITY AUTHORIZATION

Control: The organization:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;

b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and

c. Updates the security authorization **if the organization and/or system is adequately covered by a continuous monitoring program the Security Authorization may be continuously updated: If not; at least every three (3) years, when significant security breaches occur, whenever there is a significant change to the system, or to the environment in which the system operates**.

Supplemental Guidance: Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. The security authorization process is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions. Related controls: CA-2, CA-7, PM-9, PM-10.

The Cybersecurity enclosure to DoDM 5205.07-V1 provides policy for assigning the AO with authority to authorize systems to operate under their purview. [CA-6.a] The ISO and ISSM/ISSO must ensure the system is authorized for processing by the AO before commencing operations.

Joint Authorization vs. Reciprocity

Joint authorization (formerly joint accreditation) to operate differs from reciprocity in that 'joint' indicates that decisions about the system, how it will operate, which controls apply, who will assess the system as well as factors related to the actual authorization assessment are all decided up-front together, or jointly. In most cases, two or more organizations support the assessment and jointly determine authorization to operate.

Reciprocity is defined as a "Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information." [CNSSI 4009]

Reciprocity applies when an information system is currently authorized to operate by one AO and it is later determined that it would prove beneficial to one or both parties if the information systems are connected or authorized to share data across system, programs, or service boundaries.

Reciprocity does not imply blind acceptance. Upon request, the body of evidence used for assessments of the subject system will be provided to the other AOs who have a vested interest in establishing a mutual agreement. The receiving party will review the assessment evidence (e.g., SSP, test plans, test procedures, test reports, exceptions) and determine if there are any deltas in the evidence, e.g., baseline/overlay controls that were tailored, a test item that was omitted and identify items that may require negotiations. Reciprocity means that the system(s) will not undergo another full assessment.

Varying security domains (collateral, SAP, sensitive compartmented information (SCI)) implement security measures based on their operating environment. A receiving organization reviews controls to ensure enhanced security measures pertinent to the receiving environment are appropriately addressed. The SSP/SCTM for a collateral system coming into a SAP environment should be reviewed and updated to reflect requirements for implementation in a SAP environment, e.g., media protection, personnel clearance and accesses, incident response and reporting, interconnections.

Organizations have the right to refuse reciprocity due to an insufficient security authorization package or excessive risk to the enclave or site as determined by the AO.

Ensure the CA SAPCO is aware of discussions concerning reciprocal agreements with entities outside of the organization, including reciprocity with the IC, other DoD SAPCOs, or the DoD Collateral Community.

Site-Based Authorization (SBA)

The AO may choose an alternate authorization approach that consolidates all systems at a location into a single management entity called a "Site." The size and bounds of each site are determined by the relationship of each system (component) to the infrastructure, command lines of authority, and the span of control of the site's ISSM. Site authorization begins with all systems at the site being assessed and authorized. The site is then authorized as a single entity and a single ATO is issued for systems falling under the Site Baseline. The ISSM may be delegated the authority to add 'like' systems or 'like' networks (i.e., for systems where not all users have a need to know), provided those systems do not extend beyond the site boundaries.

A Site IA Security Concept of Operations (CONOPS) or IA SOP, a system baseline of all approved systems, and a Site Security Architecture are the minimum documents required to be considered for SBA. These shall contain a listing of all systems covered under the site based authorization, a description of how the site complies with the requirements of this manual (i.e., RMF controls), and a wiring diagram showing external connections. The AO will be provided periodic updates to the baseline, and the continued authorization as a Site under SBA will be assessed annually in conjunction with the Security Review process.

Security Authorization Package

The ISO is responsible for submitting the Security Authorization Package to the SCA, who, in turn, submits the security authorization package to the AO. For information systems inheriting common controls for specific security capabilities, the security authorization package for the common controls or a reference to such documentation must also be included in the authorization package. When security controls are provided to an organization by an external provider (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization shall ensure the information needed by the AO to make a risk-based decision is made available by the control provider. The security authorization package will contain, at a minimum, the SSP (including the SCTM, ConMon Strategy or Plan, and RAR), SAR, and POA&M. In addition, the Security Assessment Plan may be required by the AO. The complexity of the RAR and ConMon Strategy vary by system and environment. Guidance on the level of detail required is provided by the AO/SCA. The AO may request additional documentation.

Control Enhancements: None.

References: OMB Circular A-130; OMB Memorandum 11-33; NIST Special Publications 800-37, 800-137.

CA-7 CONTINUOUS MONITORING

Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of [*Assignment: organization-defined metrics*] to be monitored;

b. Establishment of [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessments supporting such monitoring;

c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;

e. Correlation and analysis of security-related information generated by assessments and monitoring;

f. Response actions to address results of the analysis of security-related information; and

g. Reporting the security status of organization and the information system to [*Assignment: organization-defined personnel or roles*] **at least annually or when there is a significant change to the system, or to 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.

This strategy will drive the development of organizational Information Security Continuous Monitoring (ISCM) or ConMon Plans. ConMon Plan allows an organization to maintain the security authorization of its information systems over time in a highly dynamic environment with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools 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:

(1) CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT

The organization employs assessors or assessment teams with [*Assignment: organization-defined level of independence*] 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: (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 advocacy positions for the organizations acquiring their services.

(2) CONTINUOUS MONITORING | TYPES OF ASSESSMENTS

[Withdrawn: Incorporated into CA-2.]

(3) CONTINUOUS MONITORING | TREND ANALYSES

The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

Supplemental Guidance: Trend analyses can include, for example, examining recent threat information regarding the types of threat events that have occurred within the organization or across the federal government, success rates of certain types of cyber attacks, emerging vulnerabilities in information technologies, evolving social engineering techniques, results from multiple security control assessments, the effectiveness of configuration settings, and findings from Inspectors General or auditors.

References: OMB Memorandum 11-33; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts.

CA-8 PENETRATION TESTING

Control: The organization conducts penetration testing [*Assignment: organization-defined frequency*] on [*Assignment: organization-defined information systems or system components*].

Supplemental Guidance: Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12.

Control Enhancements:

(1) PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

Supplemental Guidance: Independent penetration agents or teams are individuals or groups who conduct impartial penetration testing of organizational information systems. Impartiality implies that penetration agents or teams are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the information systems that are the targets of the penetration testing. Supplemental guidance for CA-2 (1) provides additional information regarding independent assessments that can be applied to penetration testing. Related control: CA-2.

(2) PENETRATION TESTING | RED TEAM EXERCISES

The organization employs [*Assignment: organization-defined red team exercises*] to simulate attempts by adversaries to compromise organizational information systems in accordance with [*Assignment: organization-defined rules of engagement*].

Supplemental Guidance: Red team exercises extend the objectives of penetration testing by examining the security posture of organizations and their ability to implement effective cyber defenses. As such, red team exercises reflect simulated adversarial attempts to compromise organizational mission/business functions and provide a comprehensive assessment of the security state of information systems and organizations. Simulated adversarial attempts to compromise organizational missions/business functions and the information systems that support those missions/functions may include technology-focused attacks (e.g., interactions with hardware, software, or firmware components and/or mission/business processes) and social engineering-based attacks (e.g., interactions via email, telephone, shoulder surfing, or personal conversations). While penetration testing may be largely laboratory-based testing, organizations use red team exercises to provide more comprehensive assessments that reflect real-world conditions. Red team exercises can be used to improve security awareness and training and to assess levels of security control effectiveness.

References: None.

CA-9 INTERNAL SYSTEM CONNECTIONS

Control: The organization:

a. Authorizes internal connections of [*Assignment: organization-defined information system components or classes of 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.

Control Enhancements:

(1) INTERNAL SYSTEM CONNECTIONS | SECURITY COMPLIANCE CHECKS

The information system performs security compliance checks on constituent system components prior to the establishment of the internal connection.

Supplemental Guidance: Security compliance checks may include, for example, verification of the relevant baseline configuration. Related controls: CM-6.

References: None.

FAMILY: CONFIGURATION MANAGEMENT

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   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 **at least annually;** and

   2. Configuration management 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 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.

DoD SAP-specific policy and procedures related to CM are defined in the remainder of this section.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

CM-2 BASELINE CONFIGURATION

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

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). Reference Supply Chain Protection [SA-12] and the AO's recommended software approval process prior to acquisition of software. All non-US developed software requires AO approval prior to procurement.

Foreign Ownership, Control, and Influence (FOCI) review must be accomplished for any hardware/software introduction, version change or upgrade not previously approved for use on SAP systems. Hardware/software procured through non-DoD channels, or which may have a foreign origin, may only be used with an appropriate justification and AO approval.

A baseline configuration may represent different information computing environments such as development, test, and production. Organizations shall maintain a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

ISOs must ensure that software included on an IS baseline is managed. Document means of system copyright and IP compliance mechanisms within CM-10.

Control Enhancements:

(1) BASELINE CONFIGURATION | REVIEWS AND UPDATES

The organization reviews and updates the **baseline configuration of the information system:**

(a) **At least annually**;

(b) When required due to **significant or security relevant changes or security incidents occur**; and

(c) As an integral part of information system component installations and upgrades.

Supplemental Guidance: Related control: CM-5.

(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.

(3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS

The organization retains **at least two previous versions of baseline configurations of the information system** to support rollback.

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

(4) BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE

[Withdrawn: Incorporated into CM-7].

(5) BASELINE CONFIGURATION | AUTHORIZED SOFTWARE

[Withdrawn: Incorporated into CM-7].

(6) BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS

The organization maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration.

Supplemental Guidance: Establishing separate baseline configurations for development, testing, and operational environments helps protect information systems from unplanned/unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. Configurations in the test environment mirror the configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. This control enhancement requires separate configurations but not necessarily separate physical environments. Related controls: CM-4, SC-3, SC-7.

(7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS

The organization**:**

(a) Issues [*Assignment: organization-defined information systems, system components, or devices*] with [*Assignment: organization-defined configurations*] to individuals traveling to locations that the organization deems to be of significant risk; and

(b) Applies [*Assignment: organization-defined security safeguards*] to the devices when the individuals return.

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

SAP Systems leaving the facility should ensure that integrity configuration settings are applied. (Example: using Trusted Platform Module (TPM) or Secure Boot functions)

References: NIST Special Publication 800-128.

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization:

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

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

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

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

e. Retains records of configuration-controlled changes to the information system for one **(1) year or one (1) security review cycle, whichever is longer**;

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

g. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board)*] that convenes [*Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]*].

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 DoD SAP 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.

- **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 Discretionary access Control (DAC), Mandatory Access Control (MAC), Network Access Control (NAC).
- **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.
- **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 approval outlining the implementation and assessment process.

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

- Changes that modify the security support structure.
- Operating system changes (e.g., Windows 7 to Windows 10).
- Security Relevant software version upgrades (e.g., Update to Microsoft Office beyond AFT tool capabilities, firmware update for security appliances).
- Addition of security relevant software not previously approved for the systems.
- Addition of new server function.
- New hardware models
- Modification to system ports, protocols and services (PPS).
- Major vulnerabilities discovered after assessment and/or authorization.
- Changes to the confidentiality, integrity, or availability requirements (e.g., changing from a moderate impact level to high impact level).
- Changes in system encryption methods.
- Changes to interconnections.
- Changes to operating environment (e.g., external information system introduces media capability; introduction of Voice over Internet Protocol (IP) (VoIP) (classified or unclassified); foreign nationals move in next door; system is relocated).
- 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:

- Non-security relevant software version updates and/or upgrades.
- Addition of identical workstation type with approved image to an authorized system.
- Replacement of failed servers/system components with identical spares.
- 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.

A Configuration Control Board (CCB) 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 <u>any</u> software on any computer system may affect system authorization and must be evaluated and approved by the ISSM/ISSO with the local CCB.

<u>Control Enhancements</u>:

(1) CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES

The organization employs automated mechanisms to:

(a) Document proposed changes to the information system;

(b) Notify [*Assignment: organized-defined approval authorities*] of proposed changes to the information system and request change approval;

(c) Highlight proposed changes to the information system that have not been approved or disapproved by [*Assignment: organization-defined time period*];

(d) **Prohibit changes to the information system until designated approvals are received;**

(e) Document all changes to the information system; and

(f) Notify [*Assignment: organization-defined personnel*] when approved changes to the information system are completed.

(2) CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

<u>Supplemental Guidance</u>: Changes to information systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand organizational security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing

can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).

(3) CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION

The organization employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base.

(4) CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE

The organization requires an information security representative to be a member of **the configuration change control element defined in CM-3 g.**

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.

As indicated in JSIG, Section 1.5.14.q, ISSM responsibilities include serving as a member of the CCB.

(5) CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE

The information system implements [*Assignment: organization-defined security responses*] automatically if baseline configurations are changed in an unauthorized manner.

Supplemental Guidance: Security responses include, for example, halting information system processing, halting selected system functions, or issuing alerts/notifications to organizational personnel when there is an unauthorized modification of a configuration item.

(6) CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT

The organization ensures that cryptographic mechanisms used to provide **safeguarding of classified information from unauthorized access or modification** are under configuration management.

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.

CM-4 SECURITY IMPACT ANALYSIS

Control: 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, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems. Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.

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:

1. 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.

2. 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.

3. 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.

4. Legal compliance

   Licensing, copyrights, and intellectual property rights vary dependent on the software type, e.g., open source software, commercial off-the-shelf (COTS).

5. 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, LINIX), 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.

SAP 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 (IAW) CM-3. Reference CA-6.

Control Enhancements:

(1) SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS

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

Supplemental Guidance: Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines). Related controls: SA-11, SC-3, SC-7.

(2) SECURITY IMPACT ANALYSIS | VERIFICATION OF SECURITY FUNCTIONS

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

Supplemental Guidance: Implementation is this context refers to installing changed code in the operational information system. Related control: SA-11.

References: NIST Special Publication 800-128.

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.

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). Related controls: AC-3, AC-6, PE-3.

> 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.

Control Enhancements:

(1) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING

The information system enforces access restrictions and supports auditing of the enforcement actions.

Supplemental Guidance: Related controls: AU-2, AU-12, AU-6, CM-3, CM-6.

(2) ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES

The organization reviews information system changes **every 90 days or more frequently as the organization defines for high integrity systems AND at least annually or more frequently as the organization defines for low integrity and moderate integrity systems** and **when there is an incident or when planned changes have been performed** to determine whether unauthorized changes have occurred.

Supplemental Guidance: Indications that warrant review of information system changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process. Related controls: AU-6, AU-7, CM-3, CM-5, PE-6, PE-8.

(3) ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS

The information system prevents the installation of **all digitally signed software and firmware products** without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Supplemental Guidance: Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures, is a method of code authentication. Related controls: CM-7, SC-13, SI-7.

(4) ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION

The organization enforces dual authorization for implementing changes to [*Assignment: organization-defined information system components and system-level information*].

Supplemental Guidance: Organizations employ dual authorization to ensure that any changes to selected information system components and information cannot occur unless two qualified individuals implement such changes. The two individuals possess sufficient skills/expertise to determine if the proposed changes are correct implementations of approved changes. Dual authorization may also be known as two-person control. Related controls: AC-5, CM-3.

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

The organization:

(a) Limits privileges to change information system components and system-related information within a production or operational environment; and

(b) Reviews and reevaluates privileges **at least quarterly**.

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.

(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.

(7) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS

[Withdrawn: Incorporated into SI-7].

References: None.

CM-6 CONFIGURATION SETTINGS

Control: The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using **organizationally approved guides such as DoD SRGs, STIGs, NIST Security Configuration Checklists, Service specific guidance or NSA SCGs; if such a reference document is not available, the following are acceptable in descending order as available: (1) Commercially accepted practices (e.g., SANS) (2) Independent testing results (e.g., ICSA) or (3) Vendor literature** that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

c. Identifies, documents, and approves any deviations from established configuration settings for **all configurable information system components** based on [*Assignment: organization-defined operational requirements*]; and

d. Monitors and controls 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 Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4.

> The information system must conform to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment. Exceptions from the mandatory configuration settings for individual components within the IS based on explicit operational requirements require AO approval and should be revalidated by the organization IAW continuous monitoring plan.
>
> Organizations shall monitor and control changes to the configuration settings. Any detected unauthorized security-relevant configuration changes to an information system must be documented and reported as a possible incident. See also the Incident Response family.

Control Enhancements:

(1) CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*Assignment: organization-defined information system components*].

Supplemental Guidance: Related controls: CA-7, CM-4.

(2) CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES

The organization employs [*Assignment: organization-defined security safeguards*] to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].

Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected information system processing. Related controls: IR-4, SI-7.

(3) CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION

[Withdrawn: Incorporated into SI-7].

(4) CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION

[Withdrawn: Incorporated into CM-4].

References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: http://nvd.nist.gov, http://checklists.nist.gov, http://www.nsa.gov.

> Reference: DISA maintained Secure Host Baseline (SHB) repository
> https://disa.deps.mil/ext/cop/iase/dod-images/Pages/index.aspx (from a .mil domain)
> DISA STIGs: http://iase.disa.mil/stigs/Pages/index.aspx (CAC or PIV required)

CM-7 LEAST FUNCTIONALITY

Control: The organization:

a. Configures the information system to provide only essential capabilities; and

b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services*].

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.

Least functionality helps to minimize the potential for introduction of security vulnerabilities and includes, but is not limited to, disabling or uninstalling unused/unnecessary operating system (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 provide only essential capabilities. This includes allowing only the necessary ports, protocols, and services in accordance with functional needs, as defined in DoDI 8551.1, *Ports, Protocols, and Services Management (PPSM)* and DISA STIGs. This requirement must also consider the risk tolerance of the organization.
- Obtain and ensure compliance with the latest guidance regarding ports, protocols, and services.
- Configure information systems and components to disable the capability for automatic execution of code (e.g., AutoRun, AutoPlay).

Control Enhancements:

(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

The organization:

(a) Reviews the information system **at least annually or as system changes or incidents occur** to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and

(b) Disables **all functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure**.

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.

(2) LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION

The information system prevents program execution in accordance with [*Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage*].

Supplemental Guidance: Related controls: CM-8, PM-5.

Systems prevent program execution from organizationally specific locations: (e.g., removable media, temporary directory, a shared network drive, etc.)

(3) LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE

The organization ensures compliance with [*Assignment: organization-defined registration requirements for functions, ports, protocols, and services*].

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

(4) LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING

The organization:

(a) Identifies [*Assignment: organization-defined software programs not authorized to execute on the information system*];

(b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and

(c) Reviews and updates the list of unauthorized software programs **at least annually**.

Supplemental Guidance: The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as blacklisting. Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution. Related controls: CM-6, CM-8, PM-5.

(5) LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING

The organization:

(a) Identifies [*Assignment: organization-defined software programs authorized to execute on the information system*];

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

(c) Reviews and updates the list of authorized software programs **at least annually**.

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 verifying 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.

The organization develops and maintains an approved software list, for a specific information system. Change to this list is managed within CM-3.

Demonstration software is any software used for demonstrations, with the intent of being returned to the vendor and must be processed on a computer that has never processed or stored classified information.

Unauthorized software – All software must have a valid mission requirement. Types of software that are not authorized and must be waived in writing by the AO prior to introduction the SAP IS include:

- Games
- Public domain software or "shareware" which is obtained from unofficial channels (as defined by CNSSI 4009), any software not protected by copyright laws of any nation that may be freely used without permission of, or payment to

the creator, and that carries no warranties from, or liabilities to the creator.

- All software applications which have been developed outside government-approved facilities, such as those developed on personally owned computers at home or software acquired via non-government ‘bulletin boards
- Personally owned software or software purchased using employee funds (either purchased or gratuitously acquired)
- Software from unknown sources
- Illegally copied software in violation of copyright rules
- Software used for purposes other than allowed and specified in the End User License Agreement (EULA).
- Music and video or multimedia compact disks not procured through official Government channels
- Software used to conduct business outside of official government duties

References: DoD Instruction 8551.01.

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; and
4. Includes **minimally but not limited to: hardware specifications (manufacturer, type, model, serial number, physical location), software and software license information, information system/component owner, and for a networked component/device, the machine name**; and

b. Reviews and updates the information system component inventory **at least annually**

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.

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 the authority over and responsibility for each IS component should be with only one ISO (i.e., every item in the IS component inventory should fall within the authorization boundary of a single IS).

Control Enhancements:

(1) INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

(2) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE

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

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.

(3) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

The organization:

(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: [*Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]*].

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) INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION

The organization includes in the information system component inventory information, a means for identifying **minimally by position or role**, individuals responsible/accountable for administering those components.

Supplemental Guidance: Identifying individuals who are both responsible and accountable for administering information system components helps to ensure that the assigned components are properly administered and organizations can contact those individuals if some action is required (e.g., component is determined to be the source of a breach/compromise, component needs to be recalled/replaced, or component needs to be relocated).

(5) INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

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

(6) INFORMATION SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS

The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.

Supplemental Guidance: This control enhancement focuses on configuration settings established by organizations for information system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings. Related controls: CM-2, CM-6.

(7) INFORMATION SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY

The organization provides a centralized repository for the inventory of information system components.

Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. Centralized repositories of information system component inventories provide opportunities for efficiencies in accounting for organizational hardware, software, and firmware assets. Such repositories may also help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner).

(8) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING

The organization employs automated mechanisms to support tracking of information system components by geographic location.

Supplemental Guidance: The use of automated mechanisms to track the location of information system components can increase the accuracy of component inventories. Such capability may also help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions.

(9) INFORMATION SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS

The organization:

(a) Assigns **all acquired information system components** to an information system; and

(b) Receives an acknowledgement from the information system owner of this assignment.

Supplemental Guidance: Organizations determine the criteria for or types of information system components (e.g., microprocessors, motherboards, software, programmable logic controllers, and network devices) that are subject to this control enhancement. Related control: SA-4.

References: NIST Special Publication 800-128.

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.

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.

A Configuration Management Plan (CM 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:

- 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. This participation is most important at the Preliminary Design Review (PDR) and the Critical Design Review (CDR).

ISSM responsibilities include:

- Ensuring development and implementation of procedures in accordance with CM policies and procedures for authorizing the use of hardware/software on an IS.
- 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.
- Serving as a voting member on the CCB.

ISSO responsibilities include:

- Ensuring CM for IS software and hardware are maintained and documented.
- Following procedures developed by the ISSM, in accordance with CM policies and procedures, for authorizing software use prior to its implementation on a system. Any changes or modifications to hardware, software, or firmware of a system must be coordinated with the ISSM.

Control Enhancements:

(1) CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY

The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in information system development.

Supplemental Guidance: In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked to develop configuration management processes using personnel who are not directly involved in system development or integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the information system development and integration processes and configuration management processes to facilitate quality control and more effective oversight.

References: NIST Special Publication 800-128.

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.

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 a SAP environment can make licensing difficult, but system specific controls that are in place to ensure licensing is properly managed are required.

Control Enhancements:

(1) SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE

The organization establishes the following restrictions on the use of open source software: [*Assignment: organization-defined restrictions*].

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.

CM-11 USER-INSTALLED SOFTWARE

Control: The organization:

a. Establishes [*Assignment: organization-defined policies*] governing the installation of software by users;
b. Enforces software installation policies through [*Assignment: organization-defined methods*]; and
c. Monitors policy compliance at **continuous monitoring interval**.

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.

This control is not discussing the software approval process, only discussing who has installation privileges. Generally, system administrators install software; however, on systems where a user may be authorized to install identified approved software, e.g., from the system's online 'app store.'

This control implementation is also related directly to the use of whitelisting of software that is documented in CM-7 (5). If additional discussion of permissions for installation is warranted for the system it can be documented here. Software approval procedures are outlined in CM-2.

Control Enhancements:

(1) USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS

The information system alerts [*Assignment: organization-defined personnel or roles*] when the unauthorized installation of software is detected.

Supplemental Guidance: Related controls: CA-7, SI-4.

(2) USER-INSTALLED SOFTWARE | PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS

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.

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:

- Restoring information systems using alternate equipment.
- Performing some or all of the affected business processes using alternate processing (manual) means (typically acceptable for only short-term disruptions).
- Recovering information systems operations at an alternate location (typically acceptable for only long–term disruptions or those physically impacting the facility).
- 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 (CP) 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 (COOP) 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 (DRP)	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.

Plan Type	Purpose	Scope	Plan Relationship
Information System Contingency Plan (ISCP)	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 information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

Table 3-2: Types of Contingency Plans

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

b. Reviews and updates the current:

1. Contingency planning policy **at least annually**; and
2. Contingency planning 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 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.

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; and
6. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];

b. Distributes copies of the contingency plan to **key personnel or roles and organizational elements identified in the contingency plan**;

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system **at least annually**;

e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicates contingency plan changes **to key personnel and organizational elements identified in the contingency plan**; and

g. Protects the contingency plan from unauthorized disclosure and modification.

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

The availability impact level drives the level of contingency required for the system. The Information System Contingency Plan (ISCP) may be either a separate document specific to the IS, included in the SSP, or may be incorporated into a broader site contingency plan, such as the Business Continuity Plan (BCP) or Continuity of Operations Plan (COOP). ISCP development is the responsibility of the ISO.

A key step in developing an ISCP is to conduct a Business Impact Analysis (BIA). The BIA enables the organization to characterize the system components, supported mission/business functions, and interdependencies. The BIA purpose is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption. The organization can use the BIA results to determine contingency planning requirements and priorities. Results from the BIA can also be incorporated into the analysis and strategy development efforts for the organization’s COOP, BCPs, and DRP. The depth of planning and degree of detail in an ISCP is dependent on the mission criticality of each system should the system become unavailable. A simple statement as to how long a system can remain unavailable before it impacts the mission is the basic foundation of a BIA. 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, no 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.

Control Enhancements:

(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

The organization coordinates contingency plan development with organizational elements responsible for related plans.

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

(2) CONTINGENCY PLAN | CAPACITY PLANNING

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

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

(3) CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

The organization plans for the resumption of essential missions and business functions within **a time period as defined in the contingency plan** of contingency plan activation.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.

(4) CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS

The organization plans for the resumption of all missions and business functions within **a time period as defined in the contingency plan** of contingency plan activation.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of all missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.

(5) CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites). Related control: PE-12.

(6) CONTINGENCY PLAN | ALTERNATE PROCESSING / STORAGE SITE

The organization plans for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through information system restoration to primary processing and/or storage sites.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites). Related control: PE-12.

(7) CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS

The organization coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

Supplemental Guidance: When the capability of an organization to successfully carry out its core missions/business functions is dependent on external service providers, developing a timely and comprehensive contingency plan may become more challenging. In this situation, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization. Related control: SA-9.

(8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS

The organization identifies critical information system assets supporting essential missions and business functions.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets. Related controls: SA-14, SA-15.

References: Federal Continuity Directive 1; NIST Special Publication 800-34.

CP-3 CONTINGENCY TRAINING

Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

a. Within **ten (10) working 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.

Simulated events should be incorporated in the training. For example, training might include a scenario where a Category 3 hurricane (or similar natural/man-made potential disaster) is bearing down on your location. This would be a simulated event which would provide a more realistic training scenario.

Control Enhancements:

(1) CONTINGENCY TRAINING | SIMULATED EVENTS

The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

(2) CONTINGENCY TRAINING | AUTOMATED TRAINING ENVIRONMENTS

The organization employs automated mechanisms to provide a more thorough and realistic contingency training environment.

References: Federal Continuity Directive 1; NIST Special Publications 800-16, 800-50.

CP-4 CONTINGENCY PLAN TESTING

Control: The organization:

a. Tests the contingency plan for the information system **annually** using **documented tests as defined in the contingency plan** to determine the effectiveness of the plan and the organizational readiness to execute the plan;

b. Reviews the contingency plan test results; and

c. Initiates corrective actions, if needed.

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 previous two years and after action reports should be maintained for the life of the system.

Control Enhancements:

(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS

The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements. Related controls: IR-8, PM-8.

(2) CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE

The organization tests the contingency plan at the alternate processing site:

(a) To familiarize contingency personnel with the facility and available resources; and

(b) To evaluate the capabilities of the alternate processing site to support contingency operations.

Supplemental Guidance: Related control: CP-7.

(3) CONTINGENCY PLAN TESTING | AUTOMATED TESTING

The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.

Supplemental Guidance: Automated mechanisms provide more thorough and effective testing of contingency plans, for example: (i) by providing more complete coverage of contingency issues; (ii) by selecting more realistic test scenarios and environments; and (iii) by effectively stressing the information system and supported missions.

(4) CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION

The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Supplemental Guidance: Related controls: CP-10, SC-24.

References: Federal Continuity Directive 1; FIPS Publication 199; NIST Special Publications 800-34, 800-84.

CP-5 CONTINGENCY PLAN UPDATE

[Withdrawn: Incorporated into CP-2].

CP-6 ALTERNATE STORAGE SITE

Control: The organization:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and

b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Supplemental Guidance: Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-7, CP-9, CP-10, MP-4.

Control Enhancements:

(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.

(2) ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES

The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

(3) ALTERNATE STORAGE SITE | ACCESSIBILITY

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

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted. Related control: RA-3.

References: NIST Special Publication 800-34.

CP-7 ALTERNATE PROCESSING SITE

Control: The organization:

a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of **information system operations as defined in the contingency plan** for essential missions/business functions within **a time period as defined in the contingency plan** when the primary processing capabilities are unavailable;

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

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

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.

Control Enhancements:

(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.

(2) ALTERNATE PROCESSING SITE | ACCESSIBILITY

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

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Related control: RA-3.

(3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

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

(4) ALTERNATE PROCESSING SITE | PREPARATION FOR USE

The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

Supplemental Guidance: Site preparation includes, for example, establishing configuration settings for information system components at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and other logistical considerations are in place. Related controls: CM-2, CM-6.

(5) ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS

[Withdrawn: Incorporated into CP-7].

(6) ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE

The organization plans and prepares for circumstances that preclude returning to the primary processing site.

References: NIST Special Publication 800-34.

CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of **information system operations as defined in the contingency plan**] for essential missions and business functions within **a time period as defined in the contingency plan** when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Supplemental Guidance: This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements. Related controls: CP-2, CP-6, CP-7.

Control Enhancements:

(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

The organization:

(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

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

(2) TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

(3) TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS

The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/physical attacks, and errors of omission/commission. Organizations seek to reduce common susceptibilities by, for example, minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.

(4) TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN

The organization:

(a) Requires primary and alternate telecommunications service providers to have contingency plans;

(b) Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and

(c) Obtains evidence of contingency testing/training by providers [*Assignment: organization-defined frequency*].

Supplemental Guidance: Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

(5) TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING

The organization tests alternate telecommunication services [*Assignment: organization-defined frequency*].

References: NIST Special Publication 800-34; National Communications Systems Directive 3-10; Web: http://www.dhs.gov/telecommunications-service-priority-tsp.

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization:

a. Conducts backups of user-level information contained in the information system **at least weekly or as defined in the contingency plan**;

b. Conducts backups of system-level information contained in the information system **at least weekly or as defined in the contingency plan**;

c. Conducts backups of information system documentation including security-related documentation **when created, received, updated, or as defined in the contingency plan or at least annually**; and

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

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.

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: Loss of power.

- Loss of network connectivity.
- Loss or corruption of data.
- 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.

Control Enhancements:

(1) INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY

The organization tests backup information **at least monthly or as defined in the contingency plan** to verify media reliability and information integrity.

Supplemental Guidance: Related control: CP-4.

(2) INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING

The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

Supplemental Guidance: Related control: CP-4.

(3) INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION

The organization stores backup copies of [*Assignment: organization-defined critical information system software and other security-related information*] in a separate facility or in a fire-rated container that is not collocated with the operational system.

Supplemental Guidance: Critical information system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations. Related controls: CM-2, CM-8.

(4) INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION

[Withdrawn: Incorporated into CP-9].

(5) INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE

The organization transfers information system backup information to the alternate storage site [*Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives*].

Supplemental Guidance: Information system backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media.

(6) INFORMATION SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM

The organization accomplishes information system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

Supplemental Guidance: Related controls: CP-7, CP-10.

(7) INFORMATION SYSTEM BACKUP | DUAL AUTHORIZATION

The organization enforces dual authorization for the deletion or destruction of [*Assignment: organization-defined backup information*].

Supplemental Guidance: Dual authorization ensures that the deletion or destruction of backup information cannot occur unless two qualified individuals carry out the task. Individuals deleting/destroying backup information possess sufficient skills/expertise to determine if the proposed deletion/destruction of backup information reflects organizational policies and procedures. Dual authorization may also be known as two-person control. Related controls: AC-3, MP-2.

References: NIST Special Publication 800-34.

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.

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. Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures.

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

Control Enhancements:

(1) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING

[Withdrawn: Incorporated into CP-4].

(2) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY

The information system implements transaction recovery for systems that are transaction-based.

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

(3) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS

[Withdrawn: Addressed through tailoring procedures].

(4) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD

The organization provides the capability to restore information system components within [*Assignment: organization-defined restoration time-periods*] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Supplemental Guidance: Restoration of information system components includes, for example, reimaging which restores components to known, operational states. Related control: CM-2.

(5) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY

[Withdrawn: Incorporated into SI-13].

(6) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION

The organization protects backup and restoration hardware, firmware, and software.

Supplemental Guidance: Protection of backup and restoration hardware, firmware, and software components includes both physical and technical safeguards. Backup and restoration software includes, for example, router tables, compilers, and other security-relevant system software. Related controls: AC-3, AC-6, PE-3.

References: Federal Continuity Directive 1; NIST Special Publication 800-34.

CP-11 ALTERNATE COMMUNICATIONS PROTOCOLS

Control: The information system provides the capability to employ **alternate communications protocols as defined in the contingency plan** in support of maintaining continuity of operations.

Supplemental Guidance: Contingency plans and the associated training and testing for those plans, incorporate an alternate communications protocol capability as part of increasing the resilience of organizational information systems. Alternate communications protocols include, for example, switching from Transmission Control Protocol/Internet Protocol (TCP/IP) Version 4 to TCP/IP Version 6. Switching communications protocols may affect software applications and therefore, the potential side effects of introducing alternate communications protocols are analyzed prior to implementation.

Control Enhancements: None.

References: None.

CP-12 SAFE MODE

Control: The information system, when [*Assignment: organization-defined conditions*] are detected, enters a safe mode of operation with [*Assignment: organization-defined restrictions of safe mode of operation*].

Supplemental Guidance: For information systems supporting critical missions/business functions including, for example, military operations and weapons systems, civilian space operations, nuclear power plant operations, and air traffic control operations (especially real-time operational environments), organizations may choose to identify certain conditions under which those systems revert to a predefined safe mode of operation. The safe mode of operation, which can be activated automatically or manually, restricts the types of activities or operations information systems could execute when those conditions are encountered. Restriction includes, for example, allowing only certain functions that could be carried out under limited power or with reduced communications bandwidth.

Control Enhancements: None.

References: None.

CP-13 ALTERNATIVE SECURITY MECHANISMS

Control: The organization employs [*Assignment: organization-defined alternative or supplemental security mechanisms*] for satisfying [*Assignment: organization-defined security functions*] when the primary means of implementing the security function is unavailable or compromised.

Supplemental Guidance: This control supports information system resiliency and contingency planning/continuity of operations. To ensure mission/business continuity, organizations can implement alternative or supplemental security mechanisms. These mechanisms may be less effective than the primary mechanisms (e.g., not as easy to use, not as scalable, or not as secure). However, having the capability to readily employ these alternative/supplemental mechanisms enhances overall mission/business continuity that might otherwise be adversely impacted if organizational operations had to be curtailed until the primary means of implementing the functions was restored. Given the cost and level of effort required to provide such alternative capabilities, this control would typically be applied only to critical security capabilities provided by information systems, system components, or information system services. For example, an organization may issue to senior executives and system administrators one-time pads in case multifactor tokens, the organization's standard means for secure remote authentication, is compromised. Related control: CP-2.

Control Enhancements: None.

References: None.

FAMILY: IDENTIFICATION AND AUTHENTICATION

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; and

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.

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

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

Supplemental Guidance: Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.

Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. 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:

(1) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS

The information system implements multifactor authentication for network access to privileged Accounts.

Supplemental Guidance: Related control: AC-6.

Reference CYBERCOM Communications Tasking Order (CTO) 15-0102 *Implementation and Reporting of PKI*. ISOs should request AO guidance on CTO implementation prior to acquisition of products as some systems will require Public Key Infrastructure (PKI) while multi-factor authentication for privileged users may be a more appropriate solution for smaller systems.

(2) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

The information system implements multifactor authentication for network access to non-privileged accounts.

(3) IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS

The information system implements multifactor authentication for local access to privileged accounts.

Supplemental Guidance: Related control: AC-6.

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

The information system implements multifactor authentication for local access to non-privileged accounts.

(5) IDENTIFICATION AND AUTHENTICATION | GROUP AUTHENTICATION

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

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

(6) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE

The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].

Supplemental Guidance: Related control: AC-6.

(7) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE

The information system implements multifactor authentication for network access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].

(8) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

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 nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

(9) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT

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 nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

(10) IDENTIFICATION AND AUTHENTICATION | SINGLE SIGN-ON

The information system provides a single sign-on capability for [*Assignment: organization-defined list of information system accounts and services*].

Supplemental Guidance: Single sign-on enables users to log in once and gain access to multiple information system resources. Organizations consider the operational efficiencies provided by single sign-on capabilities with the increased risk from disclosures of single authenticators providing access to multiple system resources.

(11) IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE

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 [*Assignment: 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 control: AC-6.

(12) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

Supplemental Guidance: This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.

PIV example: The DoD endpoint CAC is DoD's version of a PIV card.

(13) IDENTIFICATION AND AUTHENTICATION | OUT-OF-BAND AUTHENTICATION

The information system implements [*Assignment: organization-defined out-of-band authentication*] under [*Assignment: organization-defined conditions*].

Supplemental Guidance: Out-of-band authentication (OOBA) refers to the use of two separate communication paths to identify and authenticate users or devices to an information system. The first path (i.e., the in-band path), is used to identify and authenticate users or devices, and generally is the path through which information flows. The second path (i.e., the out-of-band path) is used to independently verify the authentication and/or requested action. For example, a user authenticates via a notebook computer to a remote server to which the user desires access, and requests some action of the server via that communication path. Subsequently, the server contacts the user via the user's cell phone to verify that the requested action originated from the user. The user may either confirm the intended action to an individual on the telephone or provide an authentication code via the telephone. This type of authentication can be employed by organizations to mitigate actual or suspected man-in the-middle attacks. The conditions for activation can include, for example, suspicious activities, new threat indicators or elevated threat levels, or the impact level or classification level of information in requested transactions. Related controls: IA-10, IA-11, SC-37.

References: HSPD-12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: http://idmanagement.gov.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates **all types of devices** before establishing a **network** connection.

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., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability. 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, video and VoIP (VVOIP), desktop video teleconference (VTC) devices, etc.

Control Enhancements:

(1) DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION

The information system authenticates [*Assignment: organization-defined specific devices and/or types of devices*] before establishing [*Selection (one or more): local; remote; network*] connection using bidirectional authentication that is cryptographically based**.**

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.

(2) DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION

[Withdrawn: Incorporated into IA-3 (1)].

(3) DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION

The organization:

(a) Standardizes dynamic address allocation lease information and the lease duration assigned to devices in accordance with [*Assignment: organization-defined lease information and lease duration*]; and

(b) Audits lease information when assigned to a device.

Supplemental Guidance: DHCP-enabled clients obtaining leases for IP addresses from DHCP servers, is a typical example of dynamic address allocation for devices. Related controls: AU-2, AU-3, AU-6, AU-12.

(4) DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION

The organization ensures that device identification and authentication based on attestation is handled by [*Assignment: organization-defined configuration management process*].

Supplemental Guidance: Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. This might be determined via some cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the those patches/updates are done securely and at the same time do not disrupt the identification and authentication to other devices.

References: None.

IA-4 IDENTIFIER MANAGEMENT

Control: The organization manages information system identifiers by:

a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] 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 for [the life of the system for individuals, groups, roles]; 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., media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers)].**

Supplemental Guidance: Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices. Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.

Individual user identifiers (USERIDs) are used for identification of users on SAP 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.

Control Enhancements:

(1) IDENTIFIER MANAGEMENT | PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS

The organization prohibits the use of information system account identifiers that are the same as public identifiers for individual electronic mail accounts.

Supplemental Guidance: Prohibiting the use of information systems account identifiers that are the same as some public identifier such as the individual identifier section of an electronic mail address, makes it more difficult for adversaries to guess user identifiers on organizational information systems. Related control: AT-2.

(2) IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION

The organization requires that the registration process to receive an individual identifier includes supervisor authorization**.**

(3) IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION

The organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.

Supplemental Guidance: Requiring multiple forms of identification reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries.

(4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS

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, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor. Related control: AT-2.

Examples: john.smith.ctr, john.smith.civ, john.smith.uk

(5) IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT

The information system dynamically manages identifiers.

Supplemental Guidance: In contrast to conventional approaches to identification which presume static accounts for preregistered users, many distributed information systems including, for example, service-oriented architectures, rely on establishing identifiers at run time for entities that were previously unknown. In these situations, organizations anticipate and provision for the dynamic establishment of identifiers. Preestablished trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential. Related control: AC-16.

(6) IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT

The organization coordinates with [*Assignment: organization-defined external organizations*] for cross-organization management of identifiers**.**

Supplemental Guidance: Cross-organization identifier management provides the capability for organizations to appropriately identify individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

(7) IDENTIFIER MANAGEMENT | IN-PERSON REGISTRATION

The organization requires that the registration process to receive an individual identifier be conducted in person before a designated registration authority.

Supplemental Guidance: In-person registration reduces the likelihood of fraudulent identifiers being issued because it requires the physical presence of individuals and actual face-to-face interactions with designated registration authorities.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78.

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 ninety (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 changes.

Supplemental Guidance: Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous 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.

> Passwords must meet standards for strong passwords. Examples of situations that may require tailoring include, but are not limited to:
>
> - The password mechanism does not support strong password requirements.
> - The password is one factor of an authorized, multifactor authentication means.
> - The password is used by a system process (as opposed to an interactive user session).
>
> **Shared (Group) Password [IA-5.a and .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 or designee. 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.

Control Enhancements:

(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

The information system, for password-based authentication:

(a) Enforces minimum password complexity of:

- **At least eight (8) characters in length for non-privileged accounts and twelve (12) 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 three (3) of the following four (4) character classes:**
  - **English uppercase characters (A through Z);**
  - **English lowercase characters (a through z);**
  - **Base l0 digits (0 through 9); and**
  - **Special characters from the punctuation and extended character set (`~!@#$%^*&()_+-={}|[]\";<>?,./).**

(b) Enforces at least the following number of changed characters when new passwords are created: **a minimum of four (4) changed characters;**

(c) Stores and transmits only cryptographically-protected passwords;

(d) Enforces password minimum and maximum lifetime restrictions of **at least one (1) day lifetime minimum and 90 day lifetime maximum;**

(e) Prohibits password reuse for **a minimum of twenty-four (24) passwords** generations; and

(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

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.

> 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.

(2) AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION

The information system, for PKI-based authentication:

(a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;

(b) Enforces authorized access to the corresponding private key;

(c) Maps the authenticated identity to the account of the individual or group; and

(d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

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.

> 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)].

(3) AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION

The organization requires that the registration process to receive **UserIDs and passwords** be conducted **in person or by a trusted third party** before [*Assignment: organization-defined registration authority*] with authorization by [*Assignment: organization-defined personnel or roles*].

> The registration process to receive USERIDs and passwords should be carried out via physical face-to-face or video and desktop teleconference, to the maximum extent possible. The identity of a user receiving a password must be verified as part of initial distribution of the password, using valid government identification (i.e., common access card (CAC), driver's license, or passport). Passwords issued shall be temporary and used "one time," expiring immediately upon log-in.

For situations where face-to-face distribution is not feasible, due to location of the user in relation to the distribution agent, system access credentials may also be disseminated using one of the following methods identified below:

- Email to the user, via digitally signed and encrypted email using PKI, over a network that meets or exceeds the classification level of the network to which system access is being requested. Where PKI is not available, distribution via email with a "read receipt" or acknowledgement of receipt of email from the recipient is authorized as an acceptable alternative.
- Email to the supervisor or co-worker (when the supervisor is not available) via digitally signed and encrypted email using PKI, over a network that meets or exceeds the classification level of the network to which system access is being requested. Where PKI is not available, distribution via email with a "read receipt" or acknowledgement of receipt of email from the recipient is authorized as an acceptable alternative.
- Secure telephone, after validating the employee's personal information in the appropriate database: name, USERID, date of birth and place of birth or other agreed upon security questions. System access credentials disseminated via secure telephone shall only be distributed over a network that meets or exceeds the classification of the network to which system access is being requested.

The organization will define the process of how non-user entities are issued authenticators as appropriate.

(4) AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy requirements as defined in IA-5 (1).

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.

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.

(5) AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY

The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.

Supplemental Guidance: This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to the developers of commercial off-the-shelve information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring information systems or system components.

(6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS

The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

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

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. Organization procedures shall implement this protection. Users must take precautions when entering passwords to ensure that no unauthorized individual observes their password keystrokes. Examples for protecting individual authenticators are provided in IA-5 Supplemental Guidance above; the requirement is implemented using PL-4 and/or PS-6. [IA-5.h]

(7) AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS

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).

(8) AUTHENTICATOR MANAGEMENT | MULTIPLE INFORMATION SYSTEM ACCOUNTS

The organization implements **precautions including advising users that they must not use the same password for any of the following: Different systems with domains of differing classification levels; Access to different systems within one classification level (e.g., internal agency network and Intelink).; Different accounts with different privilege levels (e.g., user, administrator)** to manage the risk of compromise due to individuals having accounts on multiple information systems.

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.

(9) AUTHENTICATOR MANAGEMENT | CROSS-ORGANIZATION CREDENTIAL MANAGEMENT

The organization coordinates with [*Assignment: organization-defined external organizations*] for cross-organization management of credentials.

Supplemental Guidance: Cross-organization management of credentials provides the capability for organizations to appropriately authenticate individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

(10) AUTHENTICATOR MANAGEMENT | DYNAMIC CREDENTIAL ASSOCIATION

The information system dynamically provisions identities.

Supplemental Guidance: Authentication requires some form of binding between an identity and the authenticator used to confirm the identity. In conventional approaches, this binding is established by pre-provisioning both the identity and the authenticator to the information system. For example, the binding between a username (i.e., identity) and a password (i.e., authenticator) is accomplished by provisioning the identity and authenticator as a pair in the information system. New authentication techniques allow the binding between the identity and the authenticator to be implemented outside an information system. For example, with smartcard credentials, the identity and the authenticator are bound together on the card. Using these credentials, information systems can authenticate identities that have not been pre-provisioned, dynamically provisioning the identity after authentication. In these situations, organizations can anticipate the dynamic provisioning of identities. Preestablished trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

(11) AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION

The information system, for hardware token-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined token quality requirements*].

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

(12) AUTHENTICATOR MANAGEMENT | BIOMETRIC AUTHENTICATION

The information system, for biometric-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined biometric quality requirements*].

Supplemental Guidance: Unlike password-based authentication which provides exact matches of user-input passwords to stored passwords, biometric authentication does not provide such exact matches. Depending upon the type of biometric and the type of collection mechanism, there is likely to be some divergence from the presented biometric and stored biometric which serves as the basis of comparison. There will likely be both false positives and false negatives when making such comparisons. The rate at which the false accept and false reject rates are equal is known as the crossover rate. Biometric quality requirements include, for example, acceptable crossover rates, as that essentially reflects the accuracy of the biometric.

(13) AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS

The information system prohibits the use of cached authenticators after one **(1) hour**.

(14) AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES

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.

(15) AUTHENTICATOR MANAGEMENT | FICAM-APPROVED PRODUCTS AND SERVICES

The organization uses only FICAM-approved path discovery and validation products and services.

Supplemental Guidance: Federal Identity, Credential, and Access Management (FICAM)-approved path discovery and validation products and services are those products and services that have been approved through the FICAM conformance program, where applicable.

References: OMB Memoranda 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: http://idmanagement.gov.

IA-6 AUTHENTICATOR FEEDBACK

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

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.

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.

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.

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.

Control Enhancements: None.

References: FIPS Publication 140; Web: http://csrc.nist.gov/groups/STM/cmvp/index.html.

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:

(1) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

Supplemental Guidance: This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.

(2) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD-PARTY CREDENTIALS

The information system accepts only FICAM-approved third-party credentials.

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 Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels. Related control: AU-2.

(3) IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS

The organization employs only FICAM-approved information system components in [*Assignment: organization-defined information systems*] 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.

In lieu of FICAM-approved products, DoD SAPs shall use DoD-approved products.

(4) IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-ISSUED PROFILES

The information system 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.

In lieu of FICAM-approved profiles, DoD SAPs shall use DoD-approved implementations.

(5) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV-I CREDENTIALS

The information system accepts and electronically verifies Personal Identity Verification-I (PIV-I) credentials.

Supplemental Guidance: This control enhancement: (i) applies to logical and physical access control systems; and (ii) addresses Non-Federal Issuers (NFIs) of identity cards that desire to interoperate with United States Government Personal Identity Verification (PIV) information systems and that can be trusted by federal government-relying parties. The X.509 certificate policy for the Federal Bridge Certification Authority (FBCA) addresses PIV-I requirements. The PIV-I card is suitable for Assurance Level 4 as defined in OMB Memorandum 04-04 and NIST Special Publication 800-63, and multifactor authentication as defined in NIST Special Publication 800-116. PIV-I credentials are those credentials issued by a PIV-I provider whose PIV-I certificate policy maps to the Federal Bridge PIV-I Certificate Policy. A PIV-I provider is cross-certified (directly or through another PKI bridge) with the FBCA with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FBCA certificate policy. Related control: AU-2.

References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: http://idmanagement.gov.

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

Control: The organization identifies and authenticates [*Assignment: organization-defined information system services*] using [*Assignment: organization-defined security safeguards*].

Supplemental Guidance: This control supports service-oriented architectures and other distributed architectural approaches requiring the identification and authentication of information system services. In such architectures, external services often appear dynamically. Therefore, information systems should be able to determine in a dynamic manner, if external providers and associated services are authentic. Safeguards implemented by organizational information systems to validate provider and service authenticity include, for example, information or code signing, provenance graphs, and/or electronic signatures indicating or including the sources of services.

Control Enhancements:

(1) SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE

The organization ensures that service providers receive, validate, and transmit identification and authentication information.

(2) SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS

The organization ensures that identification and authentication decisions are transmitted between [*Assignment: organization-defined services*] consistent with organizational policies.

Supplemental Guidance: For distributed architectures (e.g., service-oriented architectures), the decisions regarding the validation of identification and authentication claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary to provide the identification and authentication decisions (as opposed to the actual identifiers and authenticators) to the services that need to act on those decisions. Related control: SC-8.

References: None.

IA-10 ADAPTIVE IDENTIFICATION AND AUTHENTICATION

Control: The organization requires that individuals accessing the information system employ [*Assignment: organization-defined supplemental authentication techniques or mechanisms*] under specific [*Assignment: organization-defined circumstances or situations*].

Supplemental Guidance: Adversaries may compromise individual authentication mechanisms and subsequently attempt to impersonate legitimate users. This situation can potentially occur with any authentication mechanisms employed by organizations. To address this threat, organizations may employ specific techniques/mechanisms and establish protocols to assess suspicious behavior (e.g., individuals accessing information that they do not typically access as part of their normal duties, roles, or responsibilities, accessing greater quantities of information than the individuals would routinely access, or attempting to access information from suspicious network addresses). In these situations when certain preestablished conditions or triggers occur, organizations can require selected individuals to provide additional authentication information. Another potential use for adaptive identification and authentication is to increase the strength of mechanism based on the number and/or types of records being accessed. Related controls: AU-6, SI-4.

Control Enhancements: None.

References: None.

IA-11 RE-AUTHENTICATION

Control: The organization requires users and devices to re-authenticate when [*Assignment: organization-defined circumstances or situations requiring re-authentication*].

Supplemental Guidance: In addition to the re-authentication requirements associated with session locks, organizations may require re-authentication of individuals and/or devices in other situations including, for example: (i) when authenticators change; (ii), when roles change; (iii) when security categories of information systems change; (iv), when the execution of privileged functions occurs; (v) after a fixed period of time; or (vi) periodically. Related control: AC-11.

Control Enhancements: None.

References: None.

FAMILY: INCIDENT RESPONSE

This section comprises the incident response controls for the DoD SAP Community and for all information systems under the purview of the cognizant SAP AO. When establishing an incident response program, policy, plan, and procedures; consider starting with the most likely incident to occur on your system. For most sites, this is a data spill. Once the basic procedures for training, testing, handling, monitoring, and reporting for one type of incident (e.g., data spill) are documented, the process is more easily expanded to encompass other potential incidents. Addressing Incident Handling (IR-4) for different types of incidents will likely require the most updates/changes.

Definitions commonly used in Incident Response include:

- **Event -** Any observable occurrence in a system and/or network. [CNSSI 4009]
- **Incident -** An occurrence that results in actual or potential jeopardy to the confidentially, integrity or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies. See cyber incident. See also event, security-relevant, and intrusion. [CNSSI 4009]
- **Cyber incident** – Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein. [CNSSI 4009]
- **Data spill or Spillage -** Security incident that results in the transfer of classified information onto an information system not authorized to store or process that information. [CNSSI 4009] Also referred to as exfiltration – the unauthorized transfer of data from a system. [CNSSI 4009]

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

b. Reviews and updates 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.

DoD SAP specific policy and procedures related to incident response are defined in the remainder of this section. Background information as it applies to incident response is provided throughout this section.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.

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

c. **At least annually** thereafter.

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.

> 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.
>
> 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.

Control Enhancements:

(1) INCIDENT RESPONSE TRAINING | SIMULATED EVENTS

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

> Emphasis is on simulated, e.g., table top exercises, hot-wash, lessons learned. Use of ‘live’ data (e.g., ‘controlled viruses’) must have prior approval by the AO.

(2) INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

References: NIST Special Publications 800-16, 800-50.

IR-3 INCIDENT RESPONSE TESTING

Control: The organization tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results.

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:

(1) INCIDENT RESPONSE TESTING | AUTOMATED TESTING

The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.

Supplemental Guidance: Organizations use automated mechanisms to more thoroughly and effectively test incident response capabilities, for example: (i) by providing more complete coverage of incident response issues; (ii) by selecting more realistic test scenarios and test environments; and (iii) by stressing the response capability. Related control: AT-2.

(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

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.

IR-4 INCIDENT HANDLING

Control: 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

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 organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). 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 point of contact (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.

Figure 3-1: Incident Response Life Cycle

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	**Unsuccessful 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. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders.

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.

Table 3-3: Cyber Incident and Reportable Cyber Event Categories

The terms used above aid in tracking trends. In rare instances when an incident may need to be reported (reference IR-6) outside of the DoD SAP Community, the CA SAPCO and AO will determine the appropriate category and channel for reporting. CA SAPCOs, for instance, may use a specific reporting process and terms to better address incidents in their community. 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.
d. Other ________

Event 6 Sub-category:
Unauthorized Monitoring - Any monitoring of an IS without written approval from legal or security authorities.

Control Enhancements:

(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

The organization employs automated mechanisms to support the incident handling process.

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

(2) INCIDENT HANDLING | DYNAMIC RECONFIGURATION

The organization includes dynamic reconfiguration of [*Assignment: organization-defined information system components*] as part of the incident response capability.

Supplemental Guidance: Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways. Organizations perform dynamic reconfiguration of information systems, for example, to stop attacks, to misdirect attackers, and to isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include time frames for achieving the reconfiguration of information systems in the definition of the reconfiguration capability, considering the potential need for rapid response in order to effectively address sophisticated cyber threats. Related controls: AC-2, AC-4, AC-16, CM-2, CM-3, CM-4.

(3) INCIDENT HANDLING | CONTINUITY OF OPERATIONS

The organization identifies **classes/categories as defined in CJCSM 6510.01B** and [*Assignment: organization-defined actions to take in response to classes of incidents*] 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) INCIDENT HANDLING | INFORMATION CORRELATION

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.

(5) INCIDENT HANDLING | AUTOMATIC DISABLING OF INFORMATION SYSTEM

The organization implements a configurable capability to automatically disable the information system if [*Assignment: organization-defined security violations*] are detected.

(6) INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES

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.

(7) INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION

The organization coordinates incident handling capability for insider threats across [*Assignment: organization-defined components or elements of the organization*].

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.

(8) INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS

The organization coordinates with [*Assignment: organization-defined external organizations*] to correlate and share [*Assignment: organization-defined incident 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 multitiered 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.

Incidents on SAP systems stay within SAP channels up through the SAPCO for external release. Incidents of SAP data spilled to non-SAP systems require PSO and AO notification prior to notifications outside of SAP channels.

(9) INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY

The organization employs [*Assignment: organization-defined dynamic response capabilities*] to effectively respond to security incidents.

Supplemental Guidance: This control enhancement addresses the deployment of replacement or new capabilities in a timely manner in response to security incidents (e.g., adversary actions during hostile cyber attacks). This includes capabilities implemented at the mission/business process level (e.g., activating alternative mission/business processes) and at the information system level. Related control: CP-10.

(10) INCIDENT HANDLING | SUPPLY CHAIN COORDINATION

The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain.

Supplemental Guidance: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving information system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities.

References: Executive Order 13587; NIST Special Publication 800-61.

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents.

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 SAP 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:

- 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.
- Device audit logs.
- IDS, content filtering applications, etc.

Control Enhancements:

(1) INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Supplemental Guidance: Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs) or other electronic databases of incidents. Related controls: AU-7, IR-4.

References: NIST Special Publication 800-61.

IR-6 INCIDENT REPORTING

Control: The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within **24 hours if not otherwise defined in formal organizational policy**; and

b. Reports security incident information to **the appropriate SAP Agency CIRT/CERT (see IR-4(8))**.

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5, IR-8.

In the case of a suspected incident, containment procedures must begin immediately. However, PSO/GSSO/CPSO 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., SAP data spilled onto another SAP system tends to be (although not always) less critical than SAP data spilled to an unclassified system.

The ISSM/ISSO is responsible for reporting incidents to security as well as to the AO, e.g., the ISSM/ISSO reports to the GSSO/CPSO, who in turn reports to the PSO and the PSO to the Director of Security and/or CA SAPCO. The ISSM/ISSO must also report the incident to the system DAO who in turn reports it to the AO and/or CA SAPCO. [IR-6.b] If an activity from another organization is involved, the PSO or Director of Security will provide proper notification to the organization.

Incidents in progress are classified a minimum of UNCLASSIFIED//Handle via Special Access Channels Only (U//HVSACO). The PSO should be notified via secure communications as soon as an incident has occurred or is in progress. 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. The CA SAPCO, Director of Security, and AO will determine follow-on actions.

Information system-related fraud, waste, and abuse issues should be reported to the PSO, ISO and/or ISSM/ISSO and dealt with by the organization's chain of command. Individuals also have the right to call the Fraud, Waste and Abuse Center (FWAC) hotline.

Control Enhancements:

(1) INCIDENT REPORTING | AUTOMATED REPORTING

The organization employs automated mechanisms to assist in the reporting of security incidents.

Supplemental Guidance: Related control: IR-7.

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 or SA 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, GSSO/CPSO, PSO/Director of Security, Incident Response lead (e.g., SAPCO's IA POC), DAO, and AO. Where a web-based form or email distribution is used, the responder should be cautious of the type of incident and the classification of information in the incident description and the classification of the system being used.

(2) INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS

The organization reports information system vulnerabilities associated with reported security incidents to [Assignment: organization-defined personnel or roles].

Service/Agency SAPCOs should identify an entity to provide Computer Network Defense (CND). PSOs and field reps would then report all incidents to the CND Service Provider (CNDSP) for analysis and response determination, providing guidance to the site as needed. This provides an organization-wide awareness of incidents, a broader capability for identifying trends, and the potential to share information with other organizations in the community.

(3) INCIDENT REPORTING | COORDINATION WITH SUPPLY CHAIN

The organization provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident.

Supplemental Guidance: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving information system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities. Organizations determine the appropriate information to share considering the value gained from support by 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; Web: http://www.us-cert.gov.

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 information system 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 CA SAPCO IA POC for forensics support.

Control Enhancements:

(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

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.

(2) INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS

The organization:

(a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and

(b) Identifies organizational incident response team members to the external providers.

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 CA SAPCO IA POCs. ISSM/ISSOs will provide local incident response team POCs to their CA SAPCO IA POC. The names and contact information may be provided in the SSP.

References: None.

IR-8 INCIDENT RESPONSE PLAN

Control: The organization:

a. Develops an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
8. Is reviewed and approved by **AO**;

b. Distributes copies of the incident response plan to **all personnel with a role or responsibility for implementing the incident response plan**;

c. Reviews the incident response plan **at least annually (incorporating lessons learned from past incidents)**;

d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

e. Communicates incident response plan changes to [**Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements**]; and

f. Protects the incident response plan 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 PSO 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.

IR-9 INFORMATION SPILLAGE RESPONSE

Control: The organization responds to information spills by:

a. Identifying the specific information involved in the information system contamination;

b. Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill;

c. Isolating the contaminated information system or system component;

d. Eradicating the information from the contaminated information system or component;

e. Identifying other information systems or system components that may have been subsequently contaminated; and

f. Performing other [*Assignment: organization-defined actions*].

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.

Control Enhancements:

(1) INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL

The organization assigns [*Assignment: organization-defined personnel or roles*] with responsibility for responding to information spills.

(2) INFORMATION SPILLAGE RESPONSE | TRAINING

The organization provides information spillage response training **annually**.

(3) INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS

The organization implements [*Assignment: organization-defined procedures*] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

Supplemental Guidance: Correction actions for information systems contaminated due to information spillages may be very time-consuming. During those periods, personnel may not have access to the contaminated systems, which may potentially affect their ability to conduct organizational business.

(4) INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL

The organization employs [*Assignment: organization-defined security safeguards*] for personnel exposed to information not within assigned access authorizations.

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.

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.

FAMILY: MAINTENANCE

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

b. Reviews and updates 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.

DoD SAP-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.

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 [*Assignment: organization-defined personnel or roles*] 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 the individual performing the maintenance, name of escort (if necessary), a description of the type of maintenance performed, and a list of equipment removed or replaced (including identification numbers, if applicable)** in organizational maintenance records.

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.

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, e.g., PSO/GSSO/CPSO. [MA-2.c]

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 (1) year after equipment decommissioning or disposal.

Control Enhancements:

(1) CONTROLLED MAINTENANCE | RECORD CONTENT

[Withdrawn: Incorporated into MA-2].

(2) CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES

The organization:

(a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and

(b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

Supplemental Guidance: Related controls: CA-7, MA-3.

References: None.

MA-3 MAINTENANCE TOOLS

Control: The organization approves, controls, and monitors information system maintenance tools.

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:

(1) MAINTENANCE TOOLS | INSPECT TOOLS

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Supplemental Guidance: If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling. Related control: SI-7.

(2) MAINTENANCE TOOLS | INSPECT MEDIA

The organization checks media containing **diagnostic and test programs** for malicious code before the media are used in the information system.

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.

(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

(a) Verifying that there is no organizational information contained on the equipment;

(b) Sanitizing or destroying the equipment;

(c) Retaining the equipment within the facility; or

(d) Obtaining an exemption from **PSO/GSSO/CPSO and ISSM/ISSO** explicitly authorizing removal of the equipment from the facility.

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.

(4) MAINTENANCE TOOLS | RESTRICTED TOOL USE

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.

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;

d. Maintains records for nonlocal maintenance and diagnostic activities; and

e. Terminates session and network connections when nonlocal maintenance is completed.

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:

(1) NONLOCAL MAINTENANCE | AUDITING AND REVIEW

The organization:

(a) Audits nonlocal maintenance and diagnostic sessions **as defined in the organizations formal audit policy (AU-1)**; and

(b) Reviews the records of the maintenance and diagnostic sessions.

Supplemental Guidance: Related controls: AU-2, AU-6, AU-12.

(2) NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

(3) NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION

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) NONLOCAL MAINTENANCE | AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS

The organization protects nonlocal maintenance sessions by:

(a) Employing [*Assignment: organization-defined authenticators that are replay resistant*]; and

(b) Separating the maintenance sessions from other network sessions with the information system by either:

(1) Physically separated communications paths; or

(2) Logically separated communications paths based upon encryption.

Supplemental Guidance: Related control: SC-13.

(5) NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS

The organization:

(a) Requires the approval of each nonlocal maintenance session by [*Assignment: organization-defined personnel or roles*]; and

(b) Notifies [*Assignment: organization-defined personnel or roles*] of the date and time of planned nonlocal maintenance.

Supplemental Guidance: Notification may be performed by maintenance personnel. Approval of nonlocal maintenance sessions is accomplished by organizational personnel with sufficient information security and information system knowledge to determine the appropriateness of the proposed maintenance.

(6) NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION

The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.

Supplemental Guidance: Related controls: SC-8, SC-13.

(7) NONLOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION

The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.

Supplemental Guidance: Remote disconnect 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.

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.

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:

(1) MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS

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 formal 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 formal 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

(b) 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.

(2) MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS

The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for all compartments of information on the system.

> Appropriately cleared personnel who perform maintenance or diagnostics on IS do not require an escort. Organizations are responsible for ensuring maintenance personnel are familiar with organizational security procedures to assure the proper security procedures are being followed.

Supplemental Guidance: Related control: PS-3.

(3) MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS

The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are U.S. citizens.

Supplemental Guidance: Related control: PS-3.

> Outside the U.S., where U.S. citizens are not available to perform maintenance, foreign nationals may be utilized, but only with PSO and AO approval. [MA-5(3)]

(4) MAINTENANCE PERSONNEL | FOREIGN NATIONALS

The organization ensures that:

(a) Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on classified information systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and

(b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified information systems are fully documented within Memoranda of Agreements.

Supplemental Guidance: Related control: PS-3.

(5) MAINTENANCE PERSONNEL | NONSYSTEM-RELATED MAINTENANCE

The organization ensures that non-escorted personnel performing maintenance activities not directly associated with the information system but in the physical proximity of the system, have required access authorizations.

Supplemental Guidance: Personnel performing maintenance activities in other capacities not directly related to the information system include, for example, physical plant personnel and janitorial personnel.

References: None.

MA-6 TIMELY MAINTENANCE

Control: The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined information system components*] within [*Assignment: organization-defined time period*] of failure.

Supplemental Guidance: Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place. Related controls: CM-8, CP-2, CP-7, SA-14, SA-15.

Control Enhancements:

(1) TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE

The organization performs preventive maintenance on [*Assignment: organization-defined information system components*] at [*Assignment: organization-defined time intervals*].

Supplemental Guidance: Preventive maintenance includes proactive care and servicing of organizational information systems components for the purpose of maintaining equipment and facilities in satisfactory operating condition. Such maintenance provides for the systematic inspection, tests, measurements, adjustments, parts replacement, detection, and correction of incipient failures either before they occur or before they develop into major defects. The primary goal of preventive maintenance is to avoid/mitigate the consequences of equipment failures. Preventive maintenance is designed to preserve and restore equipment reliability by replacing worn components before they actually fail. Methods of determining what preventive (or other) failure management policies to apply include, for example, original equipment manufacturer (OEM) recommendations, statistical failure records, requirements of codes, legislation, or regulations within a jurisdiction, expert opinion, maintenance that has already been conducted on similar equipment, or measured values and performance indications.

(2) TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE

The organization performs predictive maintenance on [*Assignment: organization-defined information system components*] at [*Assignment: organization-defined time intervals*].

Supplemental Guidance: Predictive maintenance, or condition-based maintenance, attempts to evaluate the condition of equipment by performing periodic or continuous (online) equipment condition monitoring. The goal of predictive maintenance is to perform maintenance at a scheduled point in time when the maintenance activity is most cost-effective and before the equipment loses performance within a threshold. The predictive component of predictive maintenance stems from the goal of predicting the future trend of the equipment's condition. This approach uses principles of statistical process control to determine at what point in the future maintenance activities will be appropriate. Most predictive maintenance inspections are performed while equipment is in service, thereby minimizing disruption of normal system operations. Predictive maintenance can result in substantial cost savings and higher system reliability. Predictive maintenance tends to include measurement of the item. To evaluate equipment condition, predictive maintenance utilizes nondestructive testing technologies such as infrared, acoustic (partial discharge and airborne ultrasonic), corona detection, vibration analysis, sound level measurements, oil analysis, and other specific online tests.

(3) TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE

The organization employs automated mechanisms to transfer predictive maintenance data to a computerized maintenance management system.

Supplemental Guidance: A computerized maintenance management system maintains a computer database of information about the maintenance operations of organizations and automates processing equipment condition data in order to trigger maintenance planning, execution, and reporting.

References: None.

FAMILY: MEDIA PROTECTION

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; and
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.

> DoD SAP-specific policy and procedures related to media protection are defined in the remainder of this section. Reference [SI-3] for scanning media for malicious code.
>
> 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.
>
> 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 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.

MP-2 MEDIA ACCESS

Control: The organization restricts access to **all types of digital and/or non-digital media** to [*Assignment: organization-defined personnel or roles*].

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.

The PSO/GSSO/CPSO provides security control measures for both digital and non-digital media. However, the term media throughout the rest of this media protection section refers to digital media as opposed to non-digital media (e.g., microfilm, paper).

All digital media, and the use of such media, must be authorized by the PSO, or designee, prior to being introduced into the SAPF. 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 SAP-accredited facilities without PSO approval.

Control Enhancements:

(1) MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS

[Withdrawn: Incorporated into MP-4 (2)].

(2) MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Incorporated into SC-28 (1)].

References: FIPS Publication 199; NIST Special Publication 800-111.

MP-3 MEDIA MARKING

Control: The organization:

a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempts **new, unused, factory-sealed media** from marking as long as the media remain within [*Assignment: organization-defined controlled areas*].

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 with the current DoD SAPCO or Service's specific guidance. Reference DoDM 5205.07-V4, Enclosure 6, Marking IS Storage Media Containing SAP Information.

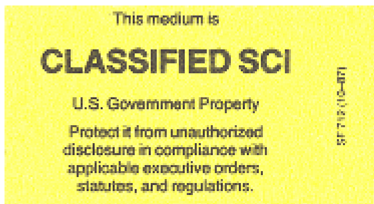
All information storage media must be appropriately marked and protected to prevent the loss of information through poor security procedures. Likewise, to prevent security compromises, all output products (to include printed material) must be appropriately marked and protected. Each user is ultimately 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 and category (e.g., TS//SAR) of the information. All information storage media will be marked with one Standard Form (SF) 700-series classification label or approved substitute and one data descriptor label or approved substitute (e.g., spreadsheet with media serial numbers and associated programs or equivalent information based on the size of the media). [MP-3(a)]

An exception to the media marking requirement is new, unused, factory-sealed media. [MP-3(b)]

Media marking labels are depicted below:



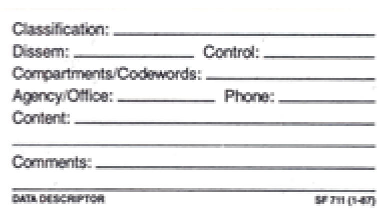
SF 712, SCI (Yellow)
Includes ALL classification levels of SCI

SF 706, TOP SECRET COLLATERAL (Orange)
Collateral Information ONLY

SF 707, SECRET COLLATERAL (Red)
Collateral Information ONLY

SF 708, CONFIDENTIAL COLLATERAL (Blue)
Collateral Information ONLY

SF 710, UNCLASSIFIED (Green)
Unclassified Information ONLY



SF 711, Data Descriptor Label

Figure 3-2: SF 700 Series Labels

Data Descriptor Label
The SF 711, Data Descriptor Label, identifies the content of a specific piece of media. A SF 711 is not required if the media labeling contains all of the information included in the SF 711.

Media Label Placement
Labels will be affixed to all media in a manner that does not adversely affect operation of the equipment in which the media is used. Labels may be trimmed to fit the media, or created specifically for this purpose so long as the colors and usage are as specified for SF 700 series

labels. 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.

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 container 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.

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.

All TS//SAR media shall be accounted for under the direct management of the Top Secret Control Officer (TSCO). For information systems with a confidentiality impact level of high, organizations shall encrypt or store off-line in a secure location information deemed to be mission-critical program hard drives and/or backup media located within a closed storage facility IAW local procedures. Program media and/or backup media located within closed storage facilities shall be protected in accordance with local procedures. [AC-3(6)] If encryption of stored information is employed as an access enforcement mechanism, the cryptography used shall be Federal Information Processing Standards Publication (FIPS Pub or FIPS) 140-2, *Security Requirements for Cryptographic Modules* (as amended), compliant. The use of encryption by the organization reduces the probability of unauthorized disclosure of information and can also detect unauthorized changes to information. Removing information from online storage to offline storage eliminates the possibility of individuals gaining unauthorized access via a network. See also SC-28.

Protection of Digital Media

As stated at the beginning of this section, CNSSI 4009 defines media as physical devices or writing surfaces including magnetic, optical, memory chips, and printouts. This section details the protection requirements for digital media which excludes paper and explains the protection afforded digital media of varying classification levels.

(a) **Accountability Systems.** When securing classified digital media, a differentiation is made between digital media that requires accountability, and that media which requires control. Accountability is very costly to the government, and is typically applied only to TS//SAR information, although on rare occasions, the Cognizant Security Authority may mandate similar procedures for S//SAR programs within the program's SCG. An appointed TSCO tracks media under this category as part of the facility Top Secret Control Account (TSCA). Accountability controls include very stringent tracking mechanisms and logs, tracking sheets which may require signatures of those who handle the media, transmission, disposition and destruction records, as well as annual inventories and account audits by a disinterested party. Reference DoDM 5205.07-V1, Enclosure 5.

(b) **Control Systems.** S//SAR and below digital media does not require the same stringent controls that are applied to accountability systems for TS although the concern for its protection and usage within the SAP facility are just as important. Unlike accountability, control systems and procedures require a tracking mechanism. Reference DoDM 5205.07-V1, Enclosure 5.

(c) **Commercial Software Protection.** 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.

(d) **Factory Fresh Media.** Factory-sealed media does not need to be controlled until opened. Once opened, this media must be brought under control and stored within the SAPF in a locked cabinet under the control of the Media Custodian. At no time will any other users be permitted to have free access to blank media.

Removable Media Accountability

ISSM/ISSO shall:

- Determine which authorized use privileges a user may have for removable media based on the user's assigned duties.
- Ensure procedures are in place to address reporting a loss of removable media and mitigating risk associated with the loss.

Each organization will audit information storage media accountability records for accuracy at least annually or as specified by the AO. The results of these audits shall be documented in an internal report to remain on file within the organization for at least one (1) year or one review cycle whichever is longer. Organizations must be able to demonstrate positive control and accounting of information storage media when reviewed by inspection authorities. Discrepancies shall be reported to the ISSM/ISSO for further reporting to the AO or designee, as required.

Control Enhancements:

(1) MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Incorporated into SC-28 (1)].

(2) MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS

The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Supplemental Guidance: Automated mechanisms can include, for example, keypads on the external entries to media storage areas. Related controls: AU-2, AU-9, AU-6, AU-12.

References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-111.

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 and PSO-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.

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.

> PSO 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 transmitted electronically whenever possible. When electronic transmission is not possible, movement of all media shall be coordinated through the appropriate personnel (ISSM/ISSO/GSSO/CPSO, etc.) following approved procedures. [MP-5(a)]. All digital media storing data at rest shall be encrypted. [SC-28]
>
> 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)]

Control Enhancements:

(1) MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS
[Withdrawn: Incorporated into MP-5].

(2) MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES
[Withdrawn: Incorporated into MP-5].

(3) MEDIA TRANSPORT | CUSTODIANS

The organization employs an identified custodian during transport of information system media outside of controlled areas.

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) MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

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.

MP-6 MEDIA SANITIZATION

Control: The organization:

a. Sanitizes **all digital and non-digital media** prior to disposal, release out of organizational control, or release for reuse using **IAW 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 not

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 GSSO/CPSO/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. The GSSO/CPSO shall develop media sanitization and removal procedures for PSO/AO approval. PSO/AO reviews and approves media sanitization procedures and equipment (NSA approved) prior to release/disposal or reuse of 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 or release out of SAP control, organizations shall 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 within channels at the same level or higher with an approved clearing process in place.

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 NSA's website for media destruction guidance including the current *Evaluated Products List – Degausser*. This Evaluated Products List (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:

- 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.
- 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 (2) 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.

- **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 (<140oF) 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 (CRT), 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 (5) 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.

- **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.
- **Laser Printer Drums, Belts, and Cartridges.**
  - Laser printer components containing light-sensitive elements (e.g., drums, belts, and complete cartridges) shall be sanitized before release from control.
  - 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).

- **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:

(1) MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY

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.

(2) MEDIA SANITIZATION | EQUIPMENT TESTING

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 (6) months for the first two (2) 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.

(3) MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined circumstances requiring sanitization of portable storage devices*].

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) MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION

[Withdrawn: Incorporated into MP-6].

(5) MEDIA SANITIZATION | CLASSIFIED INFORMATION

[Withdrawn: Incorporated into MP-6].

(6) MEDIA SANITIZATION | MEDIA DESTRUCTION

[Withdrawn: Incorporated into MP-6].

(7) MEDIA SANITIZATION | DUAL AUTHORIZATION

The organization enforces dual authorization for the sanitization of [*Assignment: organization-defined information system media*].

Supplemental Guidance: Organizations employ dual authorization to ensure that information system media sanitization cannot occur unless two technically qualified individuals conduct the task. Individuals sanitizing information system media possess sufficient skills/expertise to determine if the proposed sanitization reflects applicable federal/organizational standards, policies, and procedures. Dual authorization also helps to ensure that sanitization occurs as intended, both protecting against errors and false claims of having performed the sanitization actions. Dual authorization may also be known as two-person control. Related controls: AC-3, MP-2.

(8) MEDIA SANITIZATION | REMOTE PURGING / WIPING OF INFORMATION

The organization provides the capability to purge/wipe information from [*Assignment: organization-defined information systems, system components, or devices*] either remotely or under the following conditions: [*Assignment: organization-defined conditions*].

Supplemental Guidance: This control enhancement protects data/information on organizational information systems, system components, or devices (e.g., mobile devices) if such systems, components, or devices are obtained by unauthorized individuals. Remote purge/wipe commands require strong authentication to mitigate the risk of unauthorized individuals purging/wiping the system/component/device. The purge/wipe function can be implemented in a variety of ways including, for example, by overwriting data/information multiple times or by destroying the key necessary to decrypt encrypted data.

References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

MP-7 MEDIA USE

Control: The organization [*Selection: restricts; prohibits*] the use of [*Assignment: organization-defined types of information system media*] on [*Assignment: organization-defined information systems or system components*] using [*Assignment: organization-defined security safeguards*].

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:

(1) MEDIA USE | PROHIBIT USE WITHOUT OWNER

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.

(2) MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA

The organization prohibits the use of sanitization-resistant media in organizational information systems.

Supplemental Guidance: Sanitation-resistance applies to the capability to purge information from media. Certain types of media do not support sanitize commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitation-resistant media include, for example, compact flash, embedded flash on boards and devices, solid state drives, and USB removable media. Related control: MP-6.

References: FIPS Publication 199; NIST Special Publication 800-111.

MP-8 MEDIA DOWNGRADING

Control: The organization:

a. Establishes [*Assignment: organization-defined information system media downgrading process*] that includes employing downgrading mechanisms with [*Assignment: organization-defined strength and integrity*];

b. Ensures that the information system 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 [*Assignment: organization-defined information system media requiring downgrading*]; and

d. Downgrades the identified information system 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:

(1) MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS

The organization documents information system media downgrading actions.

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.

(2) MEDIA DOWNGRADING | EQUIPMENT TESTING

The organization employs [*Assignment: organization-defined tests*] of downgrading equipment and procedures to verify correct performance [*Assignment: organization-defined frequency*].

(3) MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION

The organization downgrades information system media containing [*Assignment: organization-defined Controlled Unclassified Information (CUI)*] prior to public release in accordance with applicable federal and organizational standards and policies.

(4) MEDIA DOWNGRADING | CLASSIFIED INFORMATION

The organization downgrades information system media containing classified information prior to release to individuals without required access authorizations in accordance with NSA standards and policies.

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 Original Classification Authority (OCA).

References: None.

FAMILY: 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. Reference also DoDM 5205.07-V3, *DoD SAP Security Manual: Physical Security Guidance for Special Access Program Facilities (SAPFs)*, April 23, 2015.

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.

DoD SAP-specific policy and procedures related to physical and environmental protection are defined in the remainder of this section. All SAPFs must be accredited (and TEMPEST certified as necessary) prior to receiving system authorization to operate. In facilities invoking OSD Memo: Approval for use of DoD SAPFs and Special Access Compartmented Areas (SAPCA) as Special Access Program Working Areas (SAPWA) for All DoD SAPs, dated December 10, 2015, security must ensure coordination with the ISSM/ISSO on situations where processing non-persistent information must be addressed. Address SCADA systems such as HVAC, fire suppression, lights and power distribution, the facility manager should work with the provider to mitigate risk to the SAP environment. Big voice systems (announcement systems) should be configured as unidirectional, i.e., not also a microphone. Ensure these systems are managed to mitigate risk associated with devices in use, e.g., disable wireless features and control access to the system/devices. Reference DoDM 5205.07-V3 and the appropriate technical specifications. Refer to DoDM 5205.07-V3 for additional information on facility accreditation and TEMPEST requirements.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100; OSD SAPWA Memo, dtd 10 Dec 2015

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 **at least annually**; and

d. Removes individuals from the facility access list when access is no longer required.

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 SAP Support Systems are controlled within a SAPF and managed by SAP cleared individuals. SAP 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.

Control Enhancements:

(1) PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION / ROLE

The organization authorizes physical access to the facility where the information system resides based on position or role.

Supplemental Guidance: Related controls: AC-2, AC-3, AC-6.

(2) PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION

The organization requires two forms of identification from [*Assignment: organization-defined list of acceptable forms of identification*] for visitor access to the facility where the information system resides.

Supplemental Guidance: Acceptable forms of government photo identification include, for example, passports, Personal Identity Verification (PIV) cards, and drivers' licenses. In the case of gaining access to facilities using automated mechanisms, organizations may use PIV cards, key cards, PINs, and biometrics. Related controls: IA-2, IA-4, IA-5.

(3) PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS

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.

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization:

a. Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by;

1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress/egress to the facility using [*Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards*];

b. Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*];

c. Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible;

d. Escorts visitors and monitors visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and monitoring*];

e. Secures keys, combinations, and other physical access devices;

f. Inventories [*Assignment: organization-defined physical access devices*] every [*Assignment: organization-defined frequency*]; and

g. Changes combinations and keys **when first installed or used** 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:

(1) PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS

The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [*Assignment: organization-defined physical spaces containing one or more components of the information system*].

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.

(2) PHYSICAL ACCESS CONTROL | FACILITY / INFORMATION SYSTEM BOUNDARIES

The organization performs security checks [*Assignment: organization-defined frequency*] 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.

(3) PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS / ALARMS / MONITORING

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) PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS

The organization uses lockable physical casings to protect [*Assignment: organization-defined information system components*] from unauthorized physical access.

(5) PHYSICAL ACCESS CONTROL | TAMPER PROTECTION

The organization employs [*Assignment: organization-defined security safeguards*] to [*Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components*] within the information system.

Supplemental Guidance: Organizations may implement tamper detection/prevention at selected hardware components or tamper detection at some components and tamper prevention at other components. Tamper detection/prevention activities can employ many types of anti-tamper technologies including, for example, tamper-detection seals and anti-tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks. Related control: SA-12.

(6) PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING

The organization employs a penetration testing process that includes [*Assignment: organization-defined frequency*], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

Supplemental Guidance: Related controls: CA-2, CA-7.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116; ICD 704, 705; DoD Instruction 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (E-PACS); Web: http://idmanagement.gov, http://fips201ep.cio.gov.

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to [*Assignment: organization-defined information system distribution and transmission lines*] within organizational facilities using [*Assignment: organization-defined security safeguards*].

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.

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 keyboard/video/mouse (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

SAP 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 SAPFs:

- KVM switches shall be authorized via approved configuration control processes and be annotated in the appropriate system documentation.
- The AO 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 National Information Assurance Partnership (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.
- KVM switches shall be installed in facilities approved for operation of the highest classification information system by authorized SAs or maintenance personnel.
- 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.
- 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.
- 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.
- 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 and approved digraphs/trigraphs (or 'SAR') 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.
- 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.
- Data of a higher classification shall not be introduced into a system of a lower classification.
- 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.
- Users shall ensure different/unique passwords are used for each system connected

through a multi-position switch.

- 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 SAPF. 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. The following order shall be used for all KVM switches within SAPFs:

- NIPRNet
- S//REL
- Secure Internet Protocol Router Network (SIPRNet)
- S//SAR
- TS Collateral
- Coalition SCI

Control Enhancements:

(1) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS

The organization:

(a) Controls physical access to output from [*Assignment: organization-defined output devices*]; and

(b) Ensures that only authorized individuals receive output from the device.

Supplemental Guidance: Controlling physical access to selected output devices includes, for example, placing printers, copiers, and facsimile machines in controlled areas with keypad access controls or limiting access to individuals with certain types of badges.

(2) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY

The information system:

(a) Controls physical access to output from [*Assignment: organization-defined output devices*]; and

(b) Links individual identity to receipt of the output from the device.

Supplemental Guidance: Controlling physical access to selected output devices includes, for example, installing security functionality on printers, copiers, and facsimile machines that allows organizations to implement authentication (e.g., using a PIN or hardware token) on output devices prior to the release of output to individuals.

Implementation of this control for printer outputs is appropriate for environments where formal access of all users is not common.

(3) ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES

The organization marks **all output devices in facilities containing information systems that 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.

Output devices such as printers and fax machines of differing security classifications should not be placed in close proximity to one another.

If Foreign Nationals are located in a SAPF, output devices of US-only systems must be under constant observation by cleared US personnel.

References: None.

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** and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; 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:

(1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT

The organization monitors physical intrusion alarms and surveillance equipment.

(2) MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION / RESPONSES

The organization employs automated mechanisms to recognize [*Assignment: organization-defined classes/types of intrusions*] and initiate [*Assignment: organization-defined response actions*].

Supplemental Guidance: Related control: SI-4.

(3) MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE

The organization employs video surveillance of [*Assignment: organization-defined operational areas*] and retains video recordings for **at least 90 days if not otherwise defined in formal organizational policy**.

Supplemental Guidance: This control enhancement focuses on recording surveillance video for purposes of subsequent review, if circumstances so warrant (e.g., a break-in detected by other means). It does not require monitoring surveillance video although organizations may choose to do so. Note that there may be legal considerations when performing and retaining video surveillance, especially if such surveillance is in a public location.

(4) MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS

The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [*Assignment: organization-defined physical spaces containing one or more components of the information system*].

Supplemental Guidance: This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers). Related controls: PS-2, PS-3.

Implementation of this control may be appropriate for a multi-system server room supported by different system or network administrators.

References: None.

PE-7 VISITOR CONTROL

[Withdrawn: Incorporated into PE-2 and PE-3].

PE-8 VISITOR ACCESS RECORDS

Control: The organization:

a. Maintains visitor access records to the facility where the information system resides for **at least two (2) years**; and

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.

SAPFs follow DoDM 5205.07-V1 guidance for visitor records and the IC Technical Specification for ICD/ICS 705 as referenced in DoDM 5205.07-V3, which require a minimum retention of two (2) years from date of last entry.

Control Enhancements:

(1) VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW

The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

(2) VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS

[Withdrawn: Incorporated into PE-2].

References: None.

PE-9 POWER EQUIPMENT AND CABLING

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance: Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites. Related control: PE-4.

Control Enhancements:

(1) POWER EQUIPMENT AND CABLING | REDUNDANT CABLING

The organization employs redundant power cabling paths that are physically separated by [*Assignment: organization-defined distance*].

Supplemental Guidance: Physically separate, redundant power cables help to ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.

(2) POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS

The organization employs automatic voltage controls for [*Assignment: organization-defined critical information system components*].

References: None.

PE-10 EMERGENCY SHUTOFF

Control: The organization:

a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;

b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and

c. Protects emergency power shutoff capability from unauthorized activation.

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 control: PE-15.

Control Enhancements:

(1) EMERGENCY SHUTOFF | ACCIDENTAL / UNAUTHORIZED ACTIVATION

[Withdrawn: Incorporated into PE-10].

References: None.

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power*] in the event of a primary power source loss.

Supplemental Guidance: Related controls: AT-3, CP-2, CP-7.

Control Enhancements:

(1) EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY

The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Supplemental Guidance: This control enhancement can be satisfied, for example, by the use of a secondary commercial power supply or other external power supply. Long-term alternate power supplies for the information system can be either manually or automatically activated.

(2) EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED

The organization provides a long-term alternate power supply for the information system that is:

(a) Self-contained;

(b) Not reliant on external power generation; and

(c) Capable of maintaining [*Selection: minimally required operational capability; full operational capability*] in the event of an extended loss of the primary power source.

Supplemental Guidance: This control enhancement can be satisfied, for example, by the use of one or more generators with sufficient capacity to meet the needs of the organization. Long-term alternate power supplies for organizational information systems are either manually or automatically activated.

References: None.

PE-12 EMERGENCY LIGHTING

Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and 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.

Control Enhancements:

(1) EMERGENCY LIGHTING | ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.

References: None.

PE-13 FIRE PROTECTION

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

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.

Control Enhancements:

(1) FIRE PROTECTION | DETECTION DEVICES / SYSTEMS

The organization employs fire detection devices/systems for the information system that activate automatically and notify [*Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders*] in the event of a fire.

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

(2) FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to [*Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders*].

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

(3) FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION

The organization employs an automatic fire suppression capability for the information system when the facility is **not staffed on a continuous basis**.

(4) FIRE PROTECTION | INSPECTIONS

The organization ensures that the facility undergoes **at least annually** inspections by authorized and qualified inspectors and resolves identified deficiencies within **60 days**.

References: None.

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and

b. Monitors temperature and humidity levels **continuously**.

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 remote maintenance and testing (RMAT) capability are properly configured for use in a SAPF 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.

Control Enhancements:

(1) TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS

The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.

(2) TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS

The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

References: None.

PE-15 WATER DAMAGE PROTECTION

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

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.

Control Enhancements:

(1) WATER DAMAGE PROTECTION | AUTOMATION SUPPORT

The organization employ**s** automated **m**echanisms to detect the presence of water in the vicinity of the information system and alerts [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Automated mechanisms can include, for example, water detection sensors, alarms, and notification systems.

References: None.

PE-16 DELIVERY AND REMOVAL

Control: The organization authorizes, monitors, and controls **all information system 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.

PE-17 ALTERNATE WORK SITE

Control: The organization:

a. Employs [*Assignment: organization-defined security controls*] at alternate work sites;

b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and

c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

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.

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The organization positions information system components within the facility to minimize potential damage from [*Assignment: organization-defined physical and environmental hazards*] and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). Related controls: CP-2, PE-19, RA-3.

When non-US systems are collocated in a SAPF, special care shall be taken to minimize the possibility of inadvertent disclosure of information and TEMPEST vulnerabilities. A CTTA shall be contacted to conduct a TEMPEST Countermeasures Review (TCR) or a TEMPEST Requirements Questionnaire (TRQ) shall be submitted. Reference PE-19

Control Enhancements:

(1) LOCATION OF INFORMATION SYSTEM COMPONENTS | FACILITY SITE

The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

Supplemental Guidance: Related control: PM-8.

References: None.

PE-19 INFORMATION LEAKAGE

Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.

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.

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. TEMPEST is a short name (not an acronym) referring to investigations and studies of compromising emanations. Reference CNSSP 300, CNSSI 7000 and NSTISSI 7001.

TEMPEST-relevant definitions include:

- **BLACK.** Designation applied to information systems, and to associated areas, circuits, components, and equipment, in which national security information is encrypted or is not processed.
- **Certified TEMPEST Technical Authority (CTTA)**. An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with CNSS approved criteria and has been appointed by a U.S. Government department or agency to fulfill CTTA responsibilities.
- **Compromising Emanations.** Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise

processed by telecommunications or automated information systems equipment.

- **Inspectable Space.** The three dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical, or where legal authority to identify and remove a potential TEMPEST exploitation exists and is exercised. CTTAs have the authority to define the inspectable space.
- **RED.** Designation applied to an IS, and associated areas, circuits, components, and equipment in which unencrypted national security information is being processed.
- **RED/BLACK Concept.** Separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (RED), in electrical form, from those that handle non-national security information (BLACK) in the same form.

TEMPEST Compliance

The CTTA will determine if there is a TEMPEST requirement and will provide the recommended TEMPEST countermeasures to the PSO. TEMPEST countermeasures may include RED/BLACK installation, facility shielding, and or/the use of TEMPEST equipment. When compliance with TEMPEST standards is required, the PSO will issue specific guidance. PSOs may refer to CNSSI 7000, *TEMPEST Countermeasures for Facilities*, and NSTISSI 7001, *NONSTOP Countermeasures*, for the criteria to have a TEMPEST Countermeasures Review performed by a CTTA. It may also be necessary to contact a CTTA to obtain the threat environment.

TEMPEST Accreditation

When TEMPEST countermeasures are directed by the PSO, TEMPEST accreditation is based on verification of the countermeasures by inspection, test, and/or analysis. Refer to DoDM 5205.07-V3 for additional information on facility accreditation and TEMPEST requirements.

TEMPEST Installation Requirements

RED/BLACK separation in accordance with CNSSAM TEMPEST/1-13 is recommended for all SAPFs when it can be performed - within manageable cost parameters.

When RED/BLACK installation is specified by the PSO for TEMPEST compliance, SAPFs will follow the installation requirements in CNSSAM TEMPEST/1-13. The TEMPEST/1-13 requirements level and specific guidance is provided by the CTTA.

Color coding or labeling that aids individuals in identifying the intended data carried by the cabling and validating its connections and proximity to emanations security concerns.

Wireless, IR, and radio devices in SAPFs must be reviewed and approved by the CA SAPCO or PSO prior to introduction into the facility.

Control Enhancements:

(1) INFORMATION LEAKAGE | NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES

The organization ensures that information system components, associated 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.

References: FIPS Publication 199.

PE-20 ASSET MONITORING AND TRACKING

Control: The organization:

a. Employs [*Assignment: organization-defined asset location technologies*] to track and monitor the location and movement of [*Assignment: organization-defined assets*] within [*Assignment: organization-defined controlled areas*]; and

b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

Supplemental Guidance: Asset location technologies can help organizations ensure that critical assets such as vehicles or essential information system components remain in authorized locations. Organizations consult with the Office of the General Counsel and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) regarding the deployment and use of asset location technologies to address potential privacy concerns. Related control: CM-8.

Control Enhancements: None.

References: None.

FAMILY: PLANNING

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; and

b. Reviews and updates the current:

1. Security planning policy **at least annually**; and
2. Security planning 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 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.

DoD SAP-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.

PL-2 SYSTEM SECURITY PLAN

Control: The organization:

a. Develops a security plan for the information system that:

1. Is consistent with the organization’s enterprise architecture;
2. Explicitly defines the authorization boundary for the system;
3. Describes the operational context of the information system in terms of missions and business processes;
4. Provides the security categorization of the information system including supporting rationale;
5. Describes the operational environment for the information system and relationships with or connections to other information systems;
6. Provides an overview of the security requirements for the system;
7. Identifies any relevant overlays, if applicable;
8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*];

c. Reviews the security plan for the information system **at least annually or when required due to system changes or modifications**;

d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

e. Protects the security plan from unauthorized disclosure and modification.

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 provides guidance on developing overlays.

Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. 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.

SAP organizations shall ensure an SSP is developed for each information system that:

- Conforms to the service/agency-accepted SSP template for SAP IS.
- Identifies the tailored controls (tailored in/out/modified) approved by the AO.
- 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.
- Is approved by the AO through coordination with the SCA prior to plan implementation

Information System Owner (ISO) Responsibilities

As stated in 1.5.12, the ISO is responsible for ensuring development and maintenance of the documentation for a security authorization package, to include the SSP and SCTM.

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.

SSP Content Classification

Oftentimes the use of Unclassified Handle Via Special Access Channels Only (U//HVSACO) is used for SSPs to preclude the disclosure of general program-related information outside established SAP channels, minimize OPSEC indicators, and facilitate communication of information within SAPs. Consult your Service/Agency representatives for proper classification guidance based upon applicable SCGs or other requirements.

Black IP addresses captured in an SSP for SAP systems are generally unclassified.

Red IP addresses captured in an SSP for SAP systems shall be protected within SAP channels.

Control Enhancements:

(1) SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS
[Withdrawn: Incorporated into PL-7].

(2) SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE
[Withdrawn: Incorporated into PL-8].

(3) SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES
The organization plans and coordinates security-related activities affecting the information system with [*Assignment: organization-defined individuals 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.

PL-3 SYSTEM SECURITY PLAN UPDATE

[Withdrawn: Incorporated into PL-2].

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 resign when the rules of behavior are revised/updated.

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:

- Reading and signing the Standard Mandatory Notice and Consent Provision for all DoD Information System User Agreements.
- Use the system for official use only. Appropriate personal use of IS must be consistent with organizational policy.
- 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.
- Observe rules and regulations governing the secure operation and authorized use of IS.
- Complete, at minimum, annual IA awareness training.
- DO NOT introduce malicious code into any IS or physically damage the system.
- 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.
- DO NOT introduce or use unauthorized software, firmware, or hardware on an IS.
- DO NOT relocate or change IS equipment or its network connectivity without proper security authorization.
- 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.
- Safeguard and report any unexpected or unrecognizable output products to the ISSO/SA as appropriate. This includes both displayed and printed products.
- 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].
- Protect IS and IS peripherals located in the user's area from unauthorized access.
- 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.
- 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.

- DO NOT tamper with access doors, covers, plates and TEMPEST seals on IS.
- Inform the appropriate ISSO/SA when access to a particular IS is no longer required (e.g., completion of project, transfer, retirement, resignation).

In addition to the requirements for a general user, privileged users shall:

- 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.
- 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.
- 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.
- Protect the "root" or "super user" authenticator at the highest level of data it secures.
- Use special accesses or permissions to perform only authorized tasks and functions.
- Take necessary precautions to protect the confidentiality of information encountered while performing privileged duties.
- Do not use special accesses or permissions to perform general user functions.
- 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:

(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS

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.

PL-5 PRIVACY IMPACT ASSESSMENT

[Withdrawn: Incorporated into Appendix J, AR-2].

PL-6 SECURITY-RELATED ACTIVITY PLANNING

[Withdrawn: Incorporated into PL-2].

PL-7 SECURITY CONCEPT OF OPERATIONS

Control: The organization:

a. Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security; and

b. Reviews and updates the CONOPS **at least annually or when changes to the information system or its environment warrant**.

Supplemental Guidance: The security CONOPS may be included in the security plan for the information system or in other system development life cycle-related documents, as appropriate. Changes to the CONOPS are reflected in ongoing updates to the security plan, the information security architecture, and other appropriate organizational documents (e.g., security specifications for procurements/acquisitions, system development life cycle documents, and systems/security engineering documents). Related control: PL-2.

The CONOPS for the information system includes, at a minimum, the purpose of the system, description of the system architecture, and data flow.

Control Enhancements: None.

References: None.

PL-8 INFORMATION SECURITY ARCHITECTURE

Control: The organization:

a. Develops an information security architecture for the information system that:

   1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

   2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and

   3. Describes any information security assumptions about, and dependencies on, external services;

b. Reviews and updates the information security architecture **at least annually or when changes to the information system or its environment warrant** to reflect updates in the enterprise architecture; and

c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

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:

(1) INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH

The organization designs its security architecture using a defense-in-depth approach that:

(a) Allocates [*Assignment: organization-defined security safeguards*] to [*Assignment: organization-defined locations and architectural layers*]; and

(b) 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.

(2) INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY

The organization requires that [*Assignment: organization-defined security safeguards*] allocated to [*Assignment: organization-defined locations and architectural layers*] 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.

PL-9 CENTRAL MANAGEMENT

Control: The organization centrally manages [*Assignment: organization-defined security controls and related processes*].

Supplemental Guidance: Central management refers to the organization-wide management and implementation of selected security controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security controls and processes. As central management of security controls is generally associated with common controls, such management promotes and facilitates standardization of security control implementations and management and judicious use of organizational resources. Centrally-managed security controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate as part of organizational continuous monitoring. As part of the security control selection process, organizations determine which controls may be suitable for central management based on organizational resources and capabilities. Organizations consider that it may not always be possible to centrally manage every aspect of a security control. In such cases, the security control is treated as a hybrid control with the control managed and implemented either centrally or at the information system level. Controls and control enhancements that are candidates for full or partial central management include, but are not limited to: AC-2 (1) (2) (3) (4); AC-17 (1) (2) (3) (9); AC-18 (1) (3) (4) (5); AC-19 (4); AC-22; AC-23; AT-2 (1) (2); AT-3 (1) (2) (3); AT-4; AU-6 (1) (3) (5) (6) (9); AU-7 (1) (2); AU-11, AU-13, AU-16, CA-2 (1) (2) (3); CA-3 (1) (2) (3); CA-7 (1); CA-9; CM-2 (1) (2); CM-3 (1) (4); CM-4; CM-6 (1); CM-7 (4) (5); CM-8 (all); CM-9 (1); CM-10; CM-11; CP-7 (all); CP-8 (all); SC-43; SI-2; SI-3; SI-7; and SI-8.

Control Enhancements: None.

References: NIST Special Publication 800-37.

FAMILY: PERSONNEL SECURITY

This section comprises the personnel security controls for the DoD SAP Community and for all information systems under the purview of the cognizant SAP AO. Reference also DoDM 5205.07-V2, *DoD SAP Security Manual: Personnel Security,* November 24, 2015.

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; and

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.

DoD SAP-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.

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 **at least annually or when the position description is updated or when the position is vacated**.

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.

OPM requires that all positions requiring access to SAP or SCI data be designated as ‘Special-Sensitive’. Access to individual SAP programs will be completed through the DoDM 5205.07-V2, Personnel Security.

Control Enhancements: None.

References: 5 C.F.R. 731.106.

PS-3 PERSONNEL SCREENING

Control: The organization:

a. Screens individuals prior to authorizing access to the information system; and

b. Rescreens individuals according to [*Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening*].

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.

Organizations shall further 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.

Control Enhancements:

(1) PERSONNEL SCREENING | CLASSIFIED INFORMATION

The organization ensures that individuals accessing an information system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

Supplemental Guidance: Related controls: AC-3, AC-4.

(2) PERSONNEL SCREENING | FORMAL INDOCTRINATION

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: Types of classified information requiring formal indoctrination include, for example, Special Access Program (SAP), Restricted Data (RD), and Sensitive Compartment Information (SCI). Related controls: AC-3, AC-4.

(3) PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES

The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

(a) Have valid access authorizations that are demonstrated by assigned official government duties; and

(b) Satisfy [*Assignment: organization-defined additional personnel screening criteria*].

Supplemental Guidance: Organizational information requiring special protection includes, for example, Controlled Unclassified Information (CUI) and Sources and Methods Information (SAMI). Personnel security criteria include, for example, position sensitivity background screening requirements.

References: 5 C.F.R. 731.106; FIPS Publications 199, 201; NIST Special Publications 800-60, 800-73, 800-76, 800-78; ICD 704.

PS-4 PERSONNEL TERMINATION

Control: The organization, upon termination of individual employment:

a. Disables information system access within**, if voluntary: as soon as possible, not to exceed 5 working days. If involuntary: Within same day as termination.**

b. Terminates/revokes any authenticators/credentials associated with the individual;

c. Conducts exit interviews that include a discussion of the non-disclosure agreement and a discussion of prohibitions against: (i) the removal of classified information from the organization's control; and (ii) direction that information be declassified in order to remove it from the organization's control;

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 [*Assignment: organization-defined personnel or roles*] within [**as soon as possible, not to exceed one (1) working day**].

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 nonavailability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.

When any system user (to include privileged and general users) leaves the organization due to employment termination or retirement, the SA 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, database access managed by another agency or organization). Reference [AC-2] and [IA-4] for additional details. Notification to the SA and the local security officer of an employee's termination shall be documented as the responsibility of the employee's supervisor or Human Resources. 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.

Control Enhancements:

(1) PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS

The organization:

(a) Notifies terminated 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.

(2) PERSONNEL TERMINATION | AUTOMATED NOTIFICATION

The organization employs automated mechanisms to notify [*Assignment: organization-defined personnel or roles*] upon termination of an individual.

Supplemental Guidance: In organizations with a large number of employees, not all personnel who need to know about termination actions receive the appropriate notifications—or, if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to specific organizational personnel or roles (e.g., management personnel, supervisors, personnel security officers, information security officers, systems administrators, or information technology administrators) when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including, for example, telephonically, via electronic mail, via text message, or via websites.

References: None.

PS-5 PERSONNEL TRANSFER

Control: The organization:

a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiates **reassignment actions to ensure all system access no longer required (need to know) are removed or disabled** within **ten (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 [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].

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.

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 to the SA 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.

Control Enhancements: None.

References: None.

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.

All users are required to read and sign a Standard Mandatory Notice and Consent provision for all DoD SAP IS, (i.e., General User Access Agreement and Acknowledgement of Responsibilities) prior to being granted access to DoD SAP information systems. In addition, privileged users are required to read and sign a DoD SAP Privileged User Access

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.

The User Access Agreement shall be retained by the ISSM/SA for a minimum of two (2) years after access is removed.

Organizations shall ensure that access to any information with special protection measures is granted only to individuals who:

- Have a valid access authorization that is demonstrated by assigned official government duties.
- Satisfy associated personnel security criteria consistent with applicable federal laws, EOs, directives, policies, regulations, standards, and guidance.
- Have read, understand, and signed a nondisclosure agreement (if applicable).

Information with special protection measures includes, for example, privacy information, proprietary information, and Sources and Methods Information (SAMI).

Control Enhancements:

(1) ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION

[Withdrawn: Incorporated into PS-3].

(2) ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION

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, Special Access Program (SAP) information, and Sensitive Compartmented Information (SCI). Personnel security criteria reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

(3) ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS

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.

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 [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within **as soon as possible, not to exceed one (1) working day**; and

e. Monitors provider compliance.

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, PSO, and/or contracting representative for clarification and guidance.

Control Enhancements: None.

References: NIST Special Publication 800-35.

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 [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

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 DoDM 5205.07-V1 and User Agreement.

Control Enhancements: None.

References: None.

FAMILY: RISK ASSESSMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to **all personnel**:

   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

b. Reviews and updates the current:

   1. Risk assessment policy **at least annually**; and

   2. Risk assessment 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 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.

DoD SAP-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.

RA-2 SECURITY CATEGORIZATION

Control: The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

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 chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted. Related controls: CM-8, MP-4, RA-3, SC-7.

Reference 2.3.1 for guidance on determining the overall security categorization, use of overlays, applicable documents, and documenting results in the SSP.

Monitoring changes to the SSP [PL-2] relates to this control.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.

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 [*Selection: security plan; risk assessment report; [Assignment: organization-defined document*]];

c. Reviews risk assessment results **at least annually**;

d. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; 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.

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. See Section 2.2.3 for a discussion of information system/authorization boundaries.

Risk assessments (either formal or informal) can be conducted by organizations at various steps in the RMF including: IS categorization; security control selection; security control implementation; security control assessment; IS authorization; and 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.

RA-4 RISK ASSESSMENT UPDATE

[Withdrawn: Incorporated into RA-3].

RA-5 VULNERABILITY SCANNING

Control: The organization:

a. Scans for vulnerabilities in the information system and hosted applications **at least quarterly** 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 [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

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 any DoD SAP systems. This information's confidentiality requires protection and access to this information must be controlled IAW Program 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 ISO is responsible for ensuring all vulnerabilities are remediated based on guidance provided by the IAVM Program or 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:

(1) VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY

The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

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.

(2) VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED

The organization updates the information system vulnerabilities scanned [*Selection (one or more):* **within 30 days prior to running scans,** *prior to a new scan; when new vulnerabilities are identified and reported*].

Supplemental Guidance: Related controls: SI-3, SI-5.

(3) VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE

The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

(4) VULNERABILITY SCANNING | DISCOVERABLE INFORMATION

The organization determines what information about the information system is discoverable by adversaries and subsequently takes [*Assignment: organization-defined corrective actions*].

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.

(5) VULNERABILITY SCANNING | PRIVILEGED ACCESS

The information system implements privileged access authorization to [*Assignment: organization-identified information system components*] for selected [*Assignment: organization-defined vulnerability scanning activities*].

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.

(6) VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

Supplemental Guidance: Related controls: IR-4, IR-5, SI-4.

(7) VULNERABILITY SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS

[Withdrawn: Incorporated into CM-8].

(8) VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS

The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

Supplemental Guidance: Related control: AU-6.

(9) VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES

[Withdrawn: Incorporated into CA-8].

(10) VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION

The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.

References: NIST Special Publications 800-40, 800-70, 800-115; Web: http://cwe.mitre.org, http://nvd.nist.gov.

RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

Control: The organization employs a technical surveillance countermeasures survey at [*Assignment: organization-defined locations*] [*Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined events or indicators occur]]*.

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.

FAMILY: SYSTEM AND SERVICES ACQUISITION

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; and

2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

b. Reviews and updates the current:

1. System and services acquisition policy **at least annually**; and

2. System and services acquisition 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 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.

DoD SAP-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.

SA-2 ALLOCATION OF RESOURCES

Control: The organization:

a. Determines information security requirements for the information system or information system service in mission/business process planning;

b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and

c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

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, Statements of Work (SOW) will include a DD Form 254 and address contractor-related security issues including, but not limited to: • Personnel security. • Physical security. • Information systems in support of the contract. • TEMPEST requirements.

- Applicable security regulations.
- Defense Federal Acquisition Regulation (DFAR) clause mandating personnel performing IA functions be certified under DoD 8570.01-M, *Information Assurance (IA) Workforce Improvement Program* or its replacement manual, DoDD 8140.01.

A Government official, either the ISSE or AO/designee, will coordinate these specific requirements depending upon the particular acquisition.

Control Enhancements: None.

References: NIST Special Publication 800-65.

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

Control: The organization:

a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;

b. Defines and documents information security roles and responsibilities throughout the system development life cycle;

c. Identifies individuals having information security roles and responsibilities; and

d. Integrates 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.

SA-4 ACQUISITION PROCESS

Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;

b. Security strength requirements;

c. Security assurance requirements;

d. Security-related documentation requirements;

e. Requirements for protecting security-related documentation;

f. Description of the information system development environment and environment in which the system is intended to operate; and

g. Acceptance criteria.

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 FISMA. Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.

Control Enhancements:

(1) ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

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.

(2) ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics;* [*Assignment: organization-defined design/implementation information*]] at [*Assignment: organization-defined 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.

(3) ACQUISITION PROCESS | DEVELOPMENT METHODS / TECHNIQUES / PRACTICES

The organization requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes [*Assignment: organization-defined state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes*].

Supplemental Guidance: Following a well-defined system development life cycle that includes state-of-the-practice software development methods, systems/security engineering methods, quality control processes, and testing, evaluation, and validation techniques helps to reduce the number and severity of latent errors within information systems, system components, and information system services. Reducing the number/severity of such errors reduces the number of vulnerabilities in those systems, components, and services. Related control: SA-12.

(4) ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS

[Withdrawn: Incorporated into CM-8 (9)].

(5) ACQUISITION PROCESS | SYSTEM / COMPONENT / SERVICE CONFIGURATIONS

The organization requires the developer of the information system, system component, or information system service to:

(a) Deliver the system, component, or service with [*Assignment: organization-defined security configurations*] implemented; and

(b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

Supplemental Guidance: Security configurations include, for example, the U.S. Government Configuration Baseline (USGCB) and any limitations on functions, ports, protocols, and services. Security characteristics include, for example, requiring that all default passwords have been changed. Related control: CM-8.

(6) ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS

The organization:

(a) Employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and

(b) Ensures 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.

(7) ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES

The organization:

(a) Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and

(b) Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.

Supplemental Guidance: Related controls: SC-12, SC-13.

(8) ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [*Assignment: organization-defined level of detail*].

Supplemental Guidance: The objective of continuous monitoring plans is to determine if the complete set of planned, required, and deployed security controls within the information system, system component, or information system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into the continuous monitoring strategies and programs implemented by organizations. Related control: CA-7.

(9) ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE

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

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.

(10) ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS

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

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.

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization:

a. Obtains administrator documentation for the information system, system component, or information system service that describes:

   1. Secure configuration, installation, and operation of the system, component, or service;

   2. Effective use and maintenance of security functions/mechanisms; and

   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

b. Obtains user documentation for the information system, system component, or information system service that describes:

1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
3. User responsibilities in maintaining the security of the system, component, or service;

c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [*Assignment: organization-defined actions*] in response;

d. Protects documentation as required, in accordance with the risk management strategy; and

e. Distributes documentation to [*Assignment: organization-defined personnel or roles*].

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. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.

Control Enhancements:

(1) INFORMATION SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS
[Withdrawn: Incorporated into SA-4 (1)].

(2) INFORMATION SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES
[Withdrawn: Incorporated into SA-4 (2)].

(3) INFORMATION SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN
[Withdrawn: Incorporated into SA-4 (2)].

(4) INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN
[Withdrawn: Incorporated into SA-4 (2)].

(5) INFORMATION SYSTEM DOCUMENTATION | SOURCE CODE
[Withdrawn: Incorporated into SA-4 (2)].

References: None.

SA-6 SOFTWARE USAGE RESTRICTIONS

[Withdrawn: Incorporated into CM-10 and SI-7].

SA-7 USER-INSTALLED SOFTWARE

[Withdrawn: Incorporated into CM-11 and SI-7].

SA-8 SECURITY ENGINEERING PRINCIPLES

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

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; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.

Systems under development or major revision shall assign an ISSE as directed by the AO. The ISSE shall be appointed in writing, and shall ensure the IS is designed, developed, and implemented with required security features and safeguards. The ISSE shall consult with the appropriate security assessor organization(s) as early as possible in the SDLC. The ISO and the respective ISSE 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.

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ [*Assignment: organization-defined security controls*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

c. Employs [*Assignment: organization-defined processes, methods, and techniques*] to monitor security control compliance by external service providers on an ongoing basis.

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:

(1) EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS

The organization:

(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and

(b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined personnel or roles*].

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.

> 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, PSO or contracting officer as appropriate based on an organization's structure.

(2) EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES

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.

(3) EXTERNAL INFORMATION SYSTEMS | ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS

The organization establishes, documents, and maintains trust relationships with external service providers based on [*Assignment: organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships*].

Supplemental Guidance: The degree of confidence that the risk from using external services is at an acceptable level depends on the trust that organizations place in the external providers, individually or in combination. Trust relationships can help organization to gain increased levels of confidence that participating service providers are providing adequate protection for the services rendered. Such relationships can be complicated due to the number of potential entities participating in the consumer-provider interactions, subordinate relationships and levels of trust, and the types of interactions between the parties. In some cases, the degree of trust is based on the amount of direct control organizations are able to exert on external service providers with regard to employment of security controls necessary for the protection of the service/information and the evidence brought forth as to the effectiveness of those controls. The level of control is typically established by the terms and conditions of the contracts or service-level agreements and can range from extensive control (e.g., negotiating contracts or agreements that specify security requirements for the providers) to very limited control (e.g., using contracts or service-level agreements to obtain commodity services such as commercial telecommunications services). In other cases, levels of trust are based on factors that convince organizations that required security controls have been employed and that determinations of control effectiveness exist. For example, separately authorized external information system services provided to organizations through well-established business relationships may provide degrees of trust in such services within the tolerable risk range of the organizations using the services. External service providers may also outsource selected services to other external entities, making the trust relationship more difficult and complicated to manage. Depending on the nature of the services, organizations may find it very difficult to place significant trust in external providers. This is not due to any inherent untrustworthiness on the part of providers, but to the intrinsic level of risk in the services.

(4) EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS

The organization employs [*Assignment: organization-defined security safeguards*] to ensure that the interests of [*Assignment: organization-defined external service providers*] are consistent with and reflect organizational interests.

Supplemental Guidance: As organizations increasingly use external service providers, the possibility exists that the interests of the service providers may diverge from organizational interests. In such situations, simply having the correct technical, procedural, or operational safeguards in place may not be sufficient if the service providers that implement and control those safeguards are not operating in a manner consistent with the interests of the consuming organizations. Possible actions that organizations might take to address such concerns include, for example, requiring background checks for selected service provider personnel, examining ownership records, employing only trustworthy service providers (i.e., providers with which organizations have had positive experiences), and conducting periodic/unscheduled visits to service provider facilities.

(5) EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION

The organization restricts the location of [*Selection (one or more): information processing; information/data; information system services*] to [*Assignment: organization-defined locations*] based on [*Assignment: organization-defined requirements or conditions*].

Supplemental Guidance: The location of information processing, information/data storage, or information system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. The criteria external providers use for the selection of processing, storage, or service locations may be different from organizational criteria. For example, organizations may want to ensure that data/information storage locations are restricted to certain locations to facilitate incident response activities (e.g., forensic analyses, after-the-fact investigations) in case of information security breaches/compromises. Such incident response activities may be adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which information system services emanate.

References: NIST Special Publication 800-35.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: The organization requires the developer of the information system, system component, or information system service to:

a. Perform configuration management during system, component, or service [**design, development, implementation, and operation**];

b. Document, manage, and control the integrity of changes to [*Assignment: organization-defined configuration items under configuration management*];

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to [*Assignment: organization-defined personnel*].

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:

(1) DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION

The organization requires the developer of the information system, system component, or information system 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.

(2) DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES

The organization provides an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

Supplemental Guidance: Alternate configuration management processes may be required, for example, when organizations use commercial off-the-shelf (COTS) information technology products. Alternate configuration management processes include organizational personnel that: (i) are responsible for reviewing/approving proposed changes to information systems, system components, and information system services; and (ii) conduct security impact analyses prior to the implementation of any changes to systems, components, or services (e.g., a configuration control board that considers security impacts of changes during development and includes representatives of both the organization and the developer, when applicable).

(3) DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of hardware components.

Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to hardware components through the use of tools, techniques, and/or mechanisms provided by developers. Organizations verify the integrity of hardware components, for example, with hard-to-copy labels and verifiable serial numbers provided by developers, and by requiring the implementation of anti-tamper technologies. Delivered hardware components also include updates to such components. Related control: SI-7.

(4) DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION

The organization requires the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions and software/firmware source and object code with previous versions.

Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components between versions during development. In contrast, SA-10 (1) and SA-10 (3) allow organizations to detect unauthorized changes to hardware, software, and firmware components through the use of tools, techniques, and/or mechanisms provided by developers.

(5) DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL

The organization requires the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components during initial development and during system life cycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs and source code) and the equivalent data in master copies on-site in operational environments is essential to ensure the availability of organizational information systems supporting critical missions and/or business functions.

(6) DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION

The organization requires the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

Supplemental Guidance: The trusted distribution of security-relevant hardware, software, and firmware updates helps to ensure that such updates are faithful representations of the master copies maintained by the developer and have not been tampered with during distribution.

References: NIST Special Publication 800-128.

SA-11 DEVELOPER SECURITY TESTING AND EVALUATION

Control: The organization requires the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan;

b. Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation at [*Assignment: organization-defined depth and coverage*];

c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during security testing/evaluation.

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

- An objective of the flaw remediation process is to correct weaknesses and deficiencies identified during the security testing and evaluation process.
- The results of the security testing/evaluation and flaw remediation process should be documented.

Control Enhancements:

(1) DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

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

(2) DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

Supplemental Guidance: Applications may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat and vulnerability analyses of information systems, system components, and information system services prior to delivery are critical to the effective operation of those systems, components, and services. Threat and vulnerability analyses at this phase of the life cycle help to ensure that design or implementation changes have been accounted for, and that any new vulnerabilities created as a result of those changes have been reviewed and mitigated. Related controls: PM-15, RA-5.

(3) DEVELOPER SECURITY TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE

The organization:

(a) Requires an independent agent satisfying [*Assignment: organization-defined independence criteria*] to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation; and

(b) Ensures that the independent agent either is provided with sufficient information to complete the verification process or has been granted the authority to obtain such information.

Supplemental Guidance: Independent agents have the necessary qualifications (i.e., expertise, skills, training, and experience) to verify the correct implementation of developer security assessment plans. Related controls: AT-3, CA-7, RA-5, SA-12.

(4) DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS

The organization requires the developer of the information system, system component, or information system service to perform a manual code review of [*Assignment: organization-defined specific code*] using [*Assignment: organization-defined processes, procedures, and/or techniques*].

Supplemental Guidance: Manual code reviews are usually reserved for the critical software and firmware components of information systems. Such code reviews are uniquely effective at identifying weaknesses that require knowledge of the application’s requirements or context which are generally unavailable to more automated analytic tools and techniques such as static or dynamic analysis. Components benefiting from manual review include for example, verifying access control matrices against application controls and reviewing more detailed aspects of cryptographic implementations and controls.

(5) DEVELOPER SECURITY TESTING AND EVALUATION | PENETRATION TESTING / ANALYSIS

The organization requires the developer of the information system, system component, or information system service to perform penetration testing at [*Assignment: organization-defined breadth/depth*] and with [*Assignment: organization-defined constraints*].

Supplemental Guidance: Penetration testing is an assessment methodology in which assessors, using all available information technology product and/or information system documentation (e.g., product/system design specifications, source code, and administrator/operator manuals) and working under specific constraints, attempt to circumvent implemented security features of information technology products and information systems. Penetration testing can include, for example, white, gray, or black box testing with analyses performed by skilled security professionals simulating adversary actions. The objective of penetration testing is to uncover potential vulnerabilities in information technology products and information systems resulting from implementation errors, configuration faults, or other operational deployment weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible.

(6) DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS

The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.

Supplemental Guidance: Attack surfaces of information systems are exposed areas that make those systems more vulnerable to cyber attacks. This includes any accessible areas where weaknesses or deficiencies in information systems (including the hardware, software, and firmware components) provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers: (i) analyze both design and implementation changes to information systems; and (ii) mitigate attack vectors generated as a result of the changes. Correction of identified flaws includes, for example, deprecation of unsafe functions.

(7) DEVELOPER SECURITY TESTING AND EVALUATION | VERIFY SCOPE OF TESTING / EVALUATION

The organization requires the developer of the information system, system component, or information system service to verify that the scope of security testing/evaluation provides complete coverage of required security controls at [*Assignment: organization-defined depth of testing/evaluation*].

Supplemental Guidance: Verifying that security testing/evaluation provides complete coverage of required security controls can be accomplished by a variety of analytic techniques ranging from informal to formal. Each of these techniques provides an increasing level of assurance corresponding to the degree of formality of the analysis. Rigorously demonstrating security control coverage at the highest levels of assurance can be provided by the use of formal modeling and analysis techniques including correlation between control implementation and corresponding test cases.

(8) DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

Supplemental Guidance: Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to help to ensure that security functionality performs in the manner in which it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies derive from the intended use of applications and the functional and design specifications for the applications. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis (checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (checking for words that are out of place in software code such as non-English language words or derogatory terms).

References: ISO/IEC 15408; NIST Special Publication 800-53A; Web: http://nvd.nist.gov, http://cwe.mitre.org, http://cve.mitre.org, http://capec.mitre.org.

SA-12 SUPPLY CHAIN PROTECTION

Control: The organization protects against supply chain threats to the information system, system component, or information system service by employing **security safeguards in accordance with CNSSD No. 505, Supply Chain Risk Management** as part of a comprehensive, defense-in-breadth 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.

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 information system components or products.

Control Enhancements:

(1) SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS

The organization employs [*Assignment: organization-defined tailored acquisition strategies, contract tools, and procurement methods*] for the purchase of the information system, system component, or information system service from suppliers.

Supplemental Guidance: The use of acquisition and procurement processes by organizations early in the system development life cycle provides an important vehicle to protect the supply chain. Organizations use available all-source intelligence analysis to inform the tailoring of acquisition strategies, tools, and methods. There are a number of different tools and techniques available (e.g., obscuring the end use of an information system or system component, using blind or filtered buys). Organizations also consider creating incentives for suppliers who: (i) implement required security safeguards; (ii) promote transparency into their organizational processes and security practices; (iii) provide additional vetting of the processes and security practices of subordinate suppliers, critical information system components, and services; (iv) restrict purchases from specific suppliers or countries; and (v) provide contract language regarding the prohibition of tainted or counterfeit components. In addition, organizations consider minimizing the time between purchase decisions and required delivery to limit opportunities for adversaries to corrupt information system components or products. Finally, organizations can use trusted/controlled distribution, delivery, and warehousing options to reduce supply chain risk (e.g., requiring tamper-evident packaging of information system components during shipping and warehousing). Related control: SA-19.

(2) SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS

The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service.

Supplemental Guidance: Supplier reviews include, for example: (i) analysis of supplier processes used to design, develop, test, implement, verify, deliver, and support information systems, system components, and information system services; and (ii) assessment of supplier training and experience in developing systems, components, or services with the required security capability. These reviews provide organizations with increased levels of visibility into supplier activities during the system development life cycle to promote more effective supply chain risk management. Supplier reviews can also help to determine whether primary suppliers have security safeguards in place and a practice for vetting subordinate suppliers, for example, second- and third-tier suppliers, and any subcontractors.

(3) SUPPLY CHAIN PROTECTION | TRUSTED SHIPPING AND WAREHOUSING

[Withdrawn: Incorporated into SA-12 (1)].

(4) SUPPLY CHAIN PROTECTION | DIVERSITY OF SUPPLIERS

[Withdrawn: Incorporated into SA-12 (13)].

(5) SUPPLY CHAIN PROTECTION | LIMITATION OF HARM

The organization employs [*Assignment: organization-defined security safeguards*] to limit harm from potential adversaries identifying and targeting the organizational supply chain.

Supplemental Guidance: Supply chain risk is part of the advanced persistent threat (APT). Security safeguards and countermeasures to reduce the probability of adversaries successfully identifying and targeting the supply chain include, for example: (i) avoiding the purchase of custom configurations to reduce the risk of acquiring information systems, components, or products that have been corrupted via supply chain actions targeted at specific organizations; (ii) employing a diverse set of suppliers to limit the potential harm from any given supplier in the supply chain; (iii) employing approved vendor lists with standing reputations in industry, and (iv) using procurement carve outs (i.e., exclusions to commitments or obligations).

(6) SUPPLY CHAIN PROTECTION | MINIMIZING PROCUREMENT TIME

[Withdrawn: Incorporated into SA-12 (1)].

(7) SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE

The organization conducts an assessment of the information system, system component, or information system service prior to selection, acceptance, or update.

Supplemental Guidance: Assessments include, for example, testing, evaluations, reviews, and analyses. Independent, third-party entities or organizational personnel conduct assessments of systems, components, products, tools, and services. Organizations conduct assessments to uncover unintentional vulnerabilities and intentional vulnerabilities including, for example, malicious code, malicious processes, defective software, and counterfeits. Assessments can include, for example, static analyses, dynamic analyses, simulations, white, gray, and black box testing, fuzz testing, penetration testing, and ensuring that components or services are genuine (e.g., using tags, cryptographic hash verifications, or digital signatures). Evidence generated during security assessments is documented for follow-on actions carried out by organizations. Related controls: CA-2, SA-11.

(8) SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE

The organization uses all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service.

Supplemental Guidance: All-source intelligence analysis is employed by organizations to inform engineering, acquisition, and risk management decisions. All-source intelligence consists of intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data in the production of finished intelligence. Where available, such information is used to analyze the risk of both intentional and unintentional vulnerabilities from development, manufacturing, and delivery processes, people, and the environment. This review is performed on suppliers at multiple tiers in the supply chain sufficient to manage risks. Related control: SA-15.

(9) SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY

The organization employs [*Assignment: organization-defined Operations Security (OPSEC) safeguards*] in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service.

Supplemental Guidance: Supply chain information includes, for example: user identities; uses for information systems, information system components, and information system services; supplier identities; supplier processes; security requirements; design specifications; testing and evaluation results; and system/component configurations. This control enhancement expands the scope of OPSEC to include suppliers and potential suppliers. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to operations and other activities to: (i) identify those actions that can be observed by potential adversaries; (ii) determine indicators that adversaries might obtain that could be interpreted or pieced together to derive critical information in sufficient time to cause harm to organizations; (iii) implement safeguards or countermeasures to eliminate or reduce to an acceptable level, exploitable vulnerabilities; and (iv) consider how aggregated information may compromise the confidentiality of users or uses of the supply chain. OPSEC may require organizations to withhold critical mission/business information from suppliers and may include the use of intermediaries to hide the end use, or users, of information systems, system components, or information system services. Related control: PE-21.

(10) SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED

The organization employs [*Assignment: organization-defined security safeguards*] to validate that the information system or system component received is genuine and has not been altered.

Supplemental Guidance: For some information system components, especially hardware, there are technical means to help determine if the components are genuine or have been altered. Security safeguards used to validate the authenticity of information systems and information system components include, for example, optical/nanotechnology tagging and side-channel analysis. For hardware, detailed bill of material information can highlight the elements with embedded logic complete with component and production location.

(11) SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS

The organization employs [*Selection (one or more): organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing*] of [*Assignment: organization-defined supply chain elements, processes, and actors*] associated with the information system, system component, or information system service.

Supplemental Guidance: This control enhancement addresses analysis and/or testing of the supply chain, not just delivered items. Supply chain elements are information technology products or product components that contain programmable logic and that are critically important to information system functions. Supply chain processes include, for example: (i) hardware, software, and firmware development processes; (ii) shipping/handling procedures; (iii) personnel and physical security programs; (iv) configuration management tools/measures to maintain provenance; or (v) any other programs, processes, or procedures associated with the production/distribution of supply chain elements. Supply chain actors are individuals with specific roles and responsibilities in the supply chain. The evidence generated during analyses and testing of supply chain elements, processes, and actors is documented and used to inform organizational risk management activities and decisions. Related control: RA-5.

(12) SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS

The organization establishes inter-organizational agreements and procedures with entities involved in the supply chain for the information system, system component, or information system service.

Supplemental Guidance: The establishment of inter-organizational agreements and procedures provides for notification of supply chain compromises. Early notification of supply chain compromises that can potentially adversely affect or have adversely affected organizational information systems, including critical system components, is essential for organizations to provide appropriate responses to such incidents.

(13) SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS

The organization employs [Assignment: organization-defined security safeguards] to ensure an adequate supply of [*Assignment: organization-defined critical information system components*].

Supplemental Guidance: Adversaries can attempt to impede organizational operations by disrupting the supply of critical information system components or corrupting supplier operations. Safeguards to ensure adequate supplies of critical information system components include, for example: (i) the use of multiple suppliers throughout the supply chain for the identified critical components; and (ii) stockpiling of spare components to ensure operation during mission-critical times.

(14) SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY

The organization establishes and retains unique identification of [*Assignment: organization-defined supply chain elements, processes, and actors*] for the information system, system component, or information system service.

Supplemental Guidance: Knowing who and what is in the supply chains of organizations is critical to gaining visibility into what is happening within such supply chains, as well as monitoring and identifying high-risk events and activities. Without reasonable visibility and traceability into supply chains (i.e., elements, processes, and actors), it is very difficult for organizations to understand and therefore manage risk, and to reduce the likelihood of adverse events. Uniquely identifying acquirer and integrator roles, organizations, personnel, mission and element processes, testing and evaluation procedures, delivery mechanisms, support mechanisms, communications/delivery paths, and disposal/final disposition activities as well as the components and tools used, establishes a foundational identity structure for assessment of supply chain activities. For example, labeling (using serial numbers) and tagging (using radio-frequency identification [RFID] tags) individual supply chain elements including software packages, modules, and hardware devices, and processes associated with those elements can be used for this purpose. Identification methods are sufficient to support the provenance in the event of a supply chain issue or adverse supply chain event.

(15) SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES

The organization establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.

Supplemental Guidance: Evidence generated during independent or organizational assessments of supply chain elements (e.g., penetration testing, audits, verification/validation activities) is documented and used in follow-on processes implemented by organizations to respond to the risks related to the identified weaknesses and deficiencies. Supply chain elements include, for example, supplier development processes and supplier distribution systems.

References: NIST Special Publication 800-161; NIST Interagency Report 7622.

Reference also CNSSD No. 505.

SA-13 TRUSTWORTHINESS

Control: The organization:

a. Describes the trustworthiness required in the [*Assignment: organization-defined information system, information system component, or information system service*] supporting its critical missions/business functions; and

b. Implements [*Assignment: organization-defined assurance overlay*] to achieve such trustworthiness.

Supplemental Guidance: This control helps organizations to make explicit trustworthiness decisions when designing, developing, and implementing information systems that are needed to conduct critical organizational missions/business functions. Trustworthiness is a characteristic/property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information it processes, stores, or transmits. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of risk despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Trustworthy systems are important to mission/business success. Two factors affecting the trustworthiness of information systems include: (i) security functionality (i.e., the security features, functions, and/or mechanisms employed within the system and its environment of operation); and (ii) security assurance (i.e., the grounds for confidence that the security functionality is effective in its application). Developers, implementers, operators, and maintainers of organizational information systems can increase the level of assurance (and trustworthiness), for example, by employing well-defined security policy models, structured and rigorous hardware, software, and firmware development techniques, sound system/security engineering principles, and secure configuration settings (defined by a set of assurance-related security controls in Appendix E).

Assurance is also based on the assessment of evidence produced during the system development life cycle. Critical missions/business functions are supported by high-impact systems and the associated assurance requirements for such systems. The additional assurance controls in Table E-4 in Appendix E (designated as optional) can be used to develop and implement high-assurance solutions for specific information systems and system components using the concept of overlays described in Appendix I. Organizations select assurance overlays that have been developed, validated, and approved for community adoption (e.g., cross-organization, government-wide), limiting the development of such overlays on an organization-by-organization basis. Organizations can conduct criticality analyses as described in SA-14, to determine the information systems, system components, or information system services that require high-assurance solutions. Trustworthiness requirements and assurance overlays can be described in the security plans for organizational information systems. Related controls: RA-2, SA-4, SA-8, SA-14, SC-3.

Control Enhancements: None.

References: FIPS Publications 199, 200; NIST Special Publications 800-53, 800-53A, 800-60, 800-64.

SA-14 CRITICALITY ANALYSIS

Control: The organization identifies critical information system components and functions by performing a criticality analysis for [*Assignment: organization-defined information systems, information system components, or information system services*] at [*Assignment: organization-defined decision points in the system development life cycle*].

Supplemental Guidance: Criticality analysis is a key tenet of supply chain risk management and informs the prioritization of supply chain protection activities such as attack surface reduction, use of all-source intelligence, and tailored acquisition strategies. Information system engineers can conduct an end-to-end functional decomposition of an information system to identify mission-critical functions and components. The functional decomposition includes the identification of core organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and beyond the information system boundary. Information system components that allow for unmediated access to critical components or functions are considered critical due to the inherent vulnerabilities such components create. Criticality is assessed in terms of the impact of the function or component failure on the ability of the component to complete the organizational missions supported by the information system. A criticality analysis is performed whenever an architecture or design is being developed or modified, including upgrades. Related controls: CP-2, PL-2, PL-8, PM-1, SA-8, SA-12, SA-13, SA-15, SA-20.

Control Enhancements: None.

(1) CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING
[Withdrawn: Incorporated into SA-20].

References: None.

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control: The organization:

a. Requires the developer of the information system, system component, or information system service to follow a documented development 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 configurations used in the development process; and
   4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Reviews the development process, standards, tools, and tool options/configurations [*Assignment: organization-defined frequency*] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [*Assignment: organization-defined 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:

(1) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | QUALITY METRICS

The organization requires the developer of the information system, system component, or information system service to:

(a) Define quality metrics at the beginning of the development process; and

(b) Provide evidence of meeting the quality metrics [*Selection (one or more): [Assignment: organization-defined frequency*]; [*Assignment: organization-defined program review milestones*]; *upon delivery*].

Supplemental Guidance: Organizations use quality metrics to establish minimum acceptable levels of information system quality. Metrics may include quality gates which are collections of completion criteria or sufficiency standards representing the satisfactory execution of particular phases of the system development project. A quality gate, for example, may require the elimination of all compiler warnings or an explicit determination that the warnings have no impact on the effectiveness of required security capabilities. During the execution phases of development projects, quality gates provide clear, unambiguous indications of progress. Other metrics apply to the entire development project. These metrics can include defining the severity thresholds of vulnerabilities, for example, requiring no known vulnerabilities in the delivered information system with a Common Vulnerability Scoring System (CVSS) severity of Medium or High.

(2) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY TRACKING TOOLS

The organization requires the developer of the information system, system component, or information system service to select and employ a security tracking tool for use during the development process.

Supplemental Guidance: Information system development teams select and deploy security tracking tools, including, for example, vulnerability/work item tracking systems that facilitate assignment, sorting, filtering, and tracking of completed work items or tasks associated with system development processes.

(3) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS

The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at [*Assignment: organization-defined breadth/depth] and at [Assignment: organization-defined decision points in the system development life cycle*].

Supplemental Guidance: This control enhancement provides developer input to the criticality analysis performed by organizations in SA-14. Developer input is essential to such analysis because organizations may not have access to detailed design documentation for information system components that are developed as commercial off-the-shelf (COTS) information technology products (e.g., functional specifications, high-level designs, low-level designs, and source code/hardware schematics). Related controls: SA-4, SA-14.

(4) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING / VULNERABILITY ANALYSIS

The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [*Assignment: organization-defined breadth/depth*] that:

(a) Uses [*Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels*];

(b) Employs [*Assignment: organization-defined tools and methods*]; and

(c) Produces evidence that meets [*Assignment: organization-defined acceptance criteria*].

Supplemental Guidance: Related control: SA-4.

(5) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION

The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to [*Assignment: organization-defined thresholds*].

Supplemental Guidance: Attack surface reduction is closely aligned with developer threat and vulnerability analyses and information system architecture and design. Attack surface reduction is a means of reducing risk to organizations by giving attackers less opportunity to exploit weaknesses or deficiencies (i.e., potential vulnerabilities) within information systems, information system components, and information system services. Attack surface reduction includes, for example, applying the principle of least privilege, employing layered defenses, applying the principle of least functionality (i.e., restricting ports, protocols, functions, and services), deprecating unsafe functions, and eliminating application programming interfaces (APIs) that are vulnerable to cyber attacks. Related control: CM-7.

(6) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT

The organization requires the developer of the information system, system component, or information system service to implement an explicit process to continuously improve the development process.

Supplemental Guidance: Developers of information systems, information system components, and information system services consider the effectiveness/efficiency of current development processes for meeting quality objectives and addressing security capabilities in current threat environments.

(7) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS

The organization requires the developer of the information system, system component, or information system service to:

(a) Perform an automated vulnerability analysis using [*Assignment: organization-defined tools*];

(b) Determine the exploitation potential for discovered vulnerabilities;

(c) Determine potential risk mitigations for delivered vulnerabilities; and

(d) Deliver the outputs of the tools and results of the analysis to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Related control: RA-5.

(8) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT / VULNERABILITY INFORMATION

The organization requires the developer of the information system, system component, or information system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.

Supplemental Guidance: Analysis of vulnerabilities found in similar software applications can inform potential design or implementation issues for information systems under development. Similar information systems or system components may exist within developer organizations. Authoritative vulnerability information is available from a variety of public and private sector sources including, for example, the National Vulnerability Database.

(9) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | USE OF LIVE DATA

The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system 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.

(10) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | INCIDENT RESPONSE PLAN

The organization requires the developer of the information system, system component, or information system service to provide an incident response plan.

Supplemental Guidance: The incident response plan for developers of information systems, system components, and information system services is incorporated into organizational incident response plans to provide the type of incident response information not readily available to organizations. Such information may be extremely helpful, for example, when organizations respond to vulnerabilities in commercial off-the-shelf (COTS) information technology products. Related control: IR-8.

(11) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ARCHIVE INFORMATION SYSTEM / COMPONENT

The organization requires the developer of the information system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security review.

Supplemental Guidance: Archiving relevant documentation from the development process can provide a readily available baseline of information that can be helpful during information system/component upgrades or modifications.

References: None.

SA-16 DEVELOPER-PROVIDED TRAINING

Control: The organization requires the developer of the information system, system component, or information system service to provide [*Assignment: organization-defined training*] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Supplemental Guidance: This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Organizations can also request sufficient training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms. Related controls: AT-2, AT-3, SA-5.

Control Enhancements: None.

References: None.

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

Control: The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;

b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and

c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Supplemental Guidance: This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to help ensure that organizations develop an information security architecture and such security architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important if/when organizations outsource the development of information systems, information system components, or information system services to external entities, and there is a requirement to demonstrate consistency with the organization's enterprise architecture and information security architecture. Related controls: PL-8, PM-7, SA-3, SA-8.

Control Enhancements:

(1) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL

The organization requires the developer of the information system, system component, or information system service to:

(a) Produce, as an integral part of the development process, a formal policy model describing the [*Assignment: organization-defined elements of organizational security policy*] to be enforced; and

(b) Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented.

Supplemental Guidance: Formal models describe specific behaviors or security policies using formal languages, thus enabling the correctness of those behaviors/policies to be formally proven. Not all components of information systems can be modeled, and generally, formal specifications are scoped to specific behaviors or policies of interest (e.g., nondiscretionary access control policies). Organizations choose the particular formal modeling language and approach based on the nature of the behaviors/policies to be described and the available tools. Formal modeling tools include, for example, Gypsy and Zed.

(2) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | SECURITY-RELEVANT COMPONENTS

The organization requires the developer of the information system, system component, or information system service to:

(a) Define security-relevant hardware, software, and firmware; and

(b) Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.

Supplemental Guidance: Security-relevant hardware, software, and firmware represent the portion of the information system, component, or service that must be trusted to perform correctly in order to maintain required security properties. Related control: SA-5.

(3) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE

The organization requires the developer of the information system, system component, or information system service to:

(a) Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;

(b) Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model;

(c) Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;

(d) Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and

(e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details present have no impact on the behaviors or policies being modeled. Formal methods can be used to show that the high-level security properties are satisfied by the formal information system description, and that the formal system description is correctly implemented by a description of some lower level, for example a hardware description. Consistency between the formal top-level specification and the formal policy models is generally not amenable to being fully proven. Therefore, a combination of formal/informal methods may be needed to show such consistency. Consistency between the formal top-level specification and the implementation may require the use of an informal demonstration due to limitations in the applicability of formal methods to prove that the specification accurately reflects the implementation. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware include, for example, mapping registers and direct memory input/output. Related control: SA-5.

(4) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE

The organization requires the developer of the information system, system component, or information system service to:

(a) Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;

(b) Show via [*Selection: informal demonstration, convincing argument with formal methods as feasible*] that the descriptive top-level specification is consistent with the formal policy model;

(c) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;

(d) Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and

(e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details present has no impact on the behaviors or policies being modeled. Consistency between the descriptive top-level specification (i.e., high-level/low-level design) and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formal/informal methods may be needed to show such consistency. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware include, for example, mapping registers and direct memory input/output. Related control: SA-5.

(5) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | CONCEPTUALLY SIMPLE DESIGN

The organization requires the developer of the information system, system component, or information system service to:

(a) Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and

(b) Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.

Supplemental Guidance: Related control: SC-3.

(6) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING

The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate testing.

Supplemental Guidance: Related control: SA-11.

(7) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE

The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.

Supplemental Guidance: Related controls: AC-5, AC-6.

References: None.

SA-18 TAMPER RESISTANCE AND DETECTION

Control: The organization implements a tamper protection program for the information system, system component, or information system service.

Supplemental Guidance: Anti-tamper technologies and techniques provide a level of protection for critical information systems, system components, and information technology products against a number of related threats including modification, reverse engineering, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting information systems, components, and products during distribution and when in use. Related controls: PE-3, SA-12, SI-7.

Control Enhancements:

(1) TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC

The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance.

Supplemental Guidance: Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations employ obfuscation and self-checking, for example, to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. Customization of information systems and system components can make substitutions easier to detect and therefore limit damage. Related control: SA-3.

(2) TAMPER RESISTANCE AND DETECTION | INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES

The organization inspects [*Assignment: organization-defined information systems, system components, or devices*] [*Selection (one or more): at random; at [Assignment: organization-defined frequency*], upon [*Assignment: organization-defined indications of need for inspection*]] to detect tampering.

Supplemental Guidance: This control enhancement addresses both physical and logical tampering and is typically applied to mobile devices, notebook computers, or other system components taken out of organization-controlled areas. Indications of need for inspection include, for example, when individuals return from travel to high-risk locations. Related control: SI-4.

References: None.

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 information system; and

b. Reports counterfeit information system components to [*Selection (one or more): source of counterfeit component*; [*Assignment: organization-defined external reporting organizations*]; [*Assignment: organization-defined personnel or roles*]].

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, SI-7.

Control Enhancements:

(1) COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING

The organization trains [*Assignment: organization-defined personnel or roles*] to detect counterfeit information system components (including hardware, software, and firmware).

(2) COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR

The organization maintains configuration control over [*Assignment: organization-defined information system components*] awaiting service/repair and serviced/repaired components awaiting return to service.

(3) COMPONENT AUTHENTICITY | COMPONENT DISPOSAL

The organization disposes of information system components using [Assignment: organization-defined techniques and methods].

Supplemental Guidance: Proper disposal of information system components helps to prevent such components from entering the gray market.

(4) COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING

The organization scans for counterfeit information system components [*Assignment: organization-defined frequency*].

References: None.

SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS

Control: The organization re-implements or custom develops [*Assignment: organization-defined critical information system components*].

Supplemental Guidance: Organizations determine that certain information system components likely cannot be trusted due to specific threats to and vulnerabilities in those components, and for which there are no viable security controls to adequately mitigate the resulting risk. Re-implementation or custom development of such components helps to satisfy requirements for higher assurance. This is accomplished by initiating changes to system components (including hardware, software, and firmware) such that the standard attacks by adversaries are less likely to succeed. In situations where no alternative sourcing is available and organizations choose not to re-implement or custom develop critical information system components, additional safeguards can be employed (e.g., enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files. Related controls: CP-2, SA-8, SA-14.

Control Enhancements: None.

References: None.

SA-21 DEVELOPER SCREENING

Control: The organization requires that the developer of [*Assignment: organization-defined information system, system component, or information system service*]:

a. Have appropriate access authorizations as determined by assigned [*Assignment: organization-defined official government duties*]; and

b. Satisfy [*Assignment: organization-defined additional personnel screening criteria*].

Supplemental Guidance: Because the information system, system component, or information system service may be employed in critical activities essential to the national and/or economic security interests of the United States, organizations have a strong interest in ensuring that the developer is trustworthy. The degree of trust required of the developer may need to be consistent with that of the individuals accessing the information system/component/service once deployed. Examples of authorization and personnel screening criteria include clearance, satisfactory background checks, citizenship, and nationality. Trustworthiness of developers may also include a review and analysis of company ownership and any relationships the company has with entities potentially affecting the quality/reliability of the systems, components, or services being developed. Related controls: PS-3, PS-7.

Control Enhancements:

(1) DEVELOPER SCREENING | VALIDATION OF SCREENING

The organization requires the developer of the information system, system component, or information system service take [*Assignment: organization-defined actions*] to ensure that the required access authorizations and screening criteria are satisfied.

Supplemental Guidance: Satisfying required access authorizations and personnel screening criteria includes, for example, providing a listing of all the individuals authorized to perform development activities on the selected information system, system component, or information system service so that organizations can validate that the developer has satisfied the necessary authorization and screening requirements.

References: None.

SA-22 UNSUPPORTED SYSTEM COMPONENTS

Control: The organization:

a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and

b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

Supplemental Guidance: Support for information system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components (e.g., when vendors are no longer providing critical software patches), provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. Related controls: PL-2, SA-3.

SA-22 is not a CNSSI 1253 baseline control, but is required to be implemented for all SAP systems. This control is non-tailorable for all SAP systems.

Control Enhancements:

(1) UNSUPPORTED SYSTEM COMPONENTS | ALTERNATIVE SOURCES FOR CONTINUED SUPPORT

The organization provides [*Selection (one or more): in-house support*; [*Assignment: organization-defined support from external providers*]] for unsupported information system components**.**

Supplemental Guidance: This control enhancement addresses the need to provide continued support for selected information system components that are no longer supported by the original developers, vendors, or manufacturers when such components remain essential to mission/business operations. Organizations can establish in-house support, for example, by developing customized patches for critical software components or secure the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include, for example, Open Source Software value-added vendors.

References: None.

SYSTEM AND SERVICES ACQUISITION CONTROLS

DEVELOPMENT OF SYSTEMS, COMPONENTS, AND SERVICES

With the renewed emphasis on trustworthy information systems and supply chain security, it is essential that organizations have the capability to express their information security requirements with clarity and specificity in order to engage the information technology industry and obtain the systems, components, and services necessary for mission and business success. To ensure that organizations have such capability, this publication provides a set of security controls in the System and Services Acquisition family (i.e., SA family) addressing requirements for the development of information systems, information technology products, and information system services. Therefore, many of the controls in the SA family are directed at developers of those systems, components, and services. It is important for organizations to recognize that the scope of the security controls in the SA family includes all system/component/service development and the developers associated with such development whether the development is conducted by internal organizational personnel or by external developers through the contracting/acquisition process. Affected controls include SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, and SA-21.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to **all personnel**:

1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates the current:

1. System and communications protection policy **at least annually if not otherwise defined in formal organizational policy**; and

2. System and communications protection procedures **at least annually if not otherwise defined in formal organizational policy**.

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.

DoD SAP-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.

SC-2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

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.

Control Enhancements:

(1) APPLICATION PARTITIONING | INTERFACES FOR NON-PRIVILEGED USERS

The information system prevents the presentation of information system management-related functionality at an interface for non-privileged users.

Supplemental Guidance: This control enhancement ensures that administration options (e.g., administrator privileges) are not available to general users (including prohibiting the use of the greyout option commonly used to eliminate accessibility to such information). Such restrictions include, for example, not presenting administration options until users establish sessions with administrator privileges. Related control: AC-3.

References: None.

SC-3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information system isolates security functions from nonsecurity 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 nonsecurity 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 nonsecurity 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.

Control Enhancements:

(1) SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION

The information system utilizes underlying hardware separation mechanisms to implement security function isolation.

Supplemental Guidance: Underlying hardware separation mechanisms include, for example, hardware ring architectures, commonly implemented within microprocessors, and hardware-enforced address segmentation used to support logically distinct storage objects with separate attributes (i.e., readable, writeable).

(2) SECURITY FUNCTION ISOLATION | ACCESS / FLOW CONTROL FUNCTIONS

The information system isolates security functions enforcing access and information flow control from nonsecurity functions and from other security functions.

Supplemental Guidance: Security function isolation occurs as a result of implementation; the functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include, for example, auditing, intrusion detection, and anti-virus functions.

(3) SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY

The organization minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.

Supplemental Guidance: In those instances where it is not feasible to achieve strict isolation of nonsecurity functions from security functions, it is necessary to take actions to minimize the nonsecurity-relevant functions within the security function boundary. Nonsecurity functions contained within the isolation boundary are considered security-relevant because errors or maliciousness in such software, by virtue of being within the boundary, can impact the security functions of organizational information systems. The design objective is that the specific portions of information systems providing information security are of minimal size/complexity. Minimizing the number of nonsecurity functions in the security-relevant components of information systems allows designers and implementers to focus only on those functions which are necessary to provide the desired security capability (typically access enforcement). By minimizing nonsecurity functions within the isolation boundaries, the amount of code that must be trusted to enforce security policies is reduced, thus contributing to understandability.

(4) SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS

The organization implements security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.

Supplemental Guidance: The reduction in inter-module interactions helps to constrain security functions and to manage complexity. The concepts of coupling and cohesion are important with respect to modularity in software design. Coupling refers to the dependencies that one module has on other modules. Cohesion refers to the relationship between the different functions within a particular module. Good software engineering practices rely on modular decomposition, layering, and minimization to reduce and manage complexity, thus producing software modules that are highly cohesive and loosely coupled.

(5) SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES

The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

Supplemental Guidance: The implementation of layered structures with minimized interactions among security functions and non-looping layers (i.e., lower-layer functions do not depend on higher-layer functions) further enables the isolation of security functions and management of complexity.

References: None.

SC-4 INFORMATION IN SHARED RESOURCES

Control: The information system 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.

Control Enhancements:

(1) INFORMATION IN SHARED RESOURCES | SECURITY LEVELS

[Withdrawn: Incorporated into SC-4].

(2) INFORMATION IN SHARED RESOURCES | PERIODS PROCESSING

The information system prevents unauthorized information transfer via shared resources in accordance with [*Assignment: organization-defined procedures*] when system processing explicitly switches between different information classification levels or security categories.

Supplemental Guidance: This control enhancement applies when there are explicit changes in information processing levels during information system operations, for example, during multilevel processing and periods processing with information at different classification levels or security categories. Organization-defined procedures may include, for example, approved sanitization processes for electronically stored information.

References: None.

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined types of denial of service attacks or reference to source for such information*] by employing [*Assignment: organization-defined security safeguards*].

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:

(1) DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS

The information system restricts the ability of individuals to launch [*Assignment: organization-defined denial of service attacks*] against other information 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.

(2) DENIAL OF SERVICE PROTECTION | EXCESS CAPACITY / BANDWIDTH / REDUNDANCY

The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.

Supplemental Guidance: Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

(3) DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING

The organization:

(a) Employs [*Assignment: organization-defined monitoring tools*] to detect indicators of denial of service attacks against the information system; and

(b) Monitors [*Assignment: organization-defined information system resources*] to determine if sufficient resources exist to prevent effective denial of service attacks.

Supplemental Guidance: Organizations consider utilization and capacity of information system resources when managing risk from denial of service due to malicious attacks. Denial of service attacks can originate from external or internal sources. Information system resources sensitive to denial of service include, for example, physical disk storage, memory, and CPU cycles. Common safeguards to prevent denial of service attacks related to storage utilization and capacity include, for example, instituting disk quotas, configuring information systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data. Related controls: CA-7, SI-4.

References: None.

SC-6 RESOURCE AVAILABILITY

Control: The information system protects the availability of resources by allocating [*Assignment: organization-defined resources*] by [*Selection (one or more); priority; quota*; [*Assignment: organization-defined security safeguards]*]].

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

Control Enhancements: None.

References: None.

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 [Selection: physically; logically] separated from internal organizational networks; and

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

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 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:

- 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.
- Route specific internal communications traffic through authenticated proxy servers within the managed interfaces of boundary protection devices, (e.g., as defined in DoDI 8551.1, *Ports, Protocols, and Services Management (PPSM)*, and DISA STIGs), 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.
- Use private/non-publicly routable IP addresses for isolated LANs.
- 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:

(1) BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS

[Withdrawn: Incorporated into SC-7].

(2) BOUNDARY PROTECTION | PUBLIC ACCESS

[Withdrawn: Incorporated into SC-7].

(3) BOUNDARY PROTECTION | ACCESS POINTS

The organization limits the number of external network connections to the information system.

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) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES

The organization:

(a) Implements a managed **interface** for each external telecommunication service;

(b) Establishes a traffic flow policy for each managed interface;

(c) Protects the confidentiality and integrity of the information being transmitted across each interface;

(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and

(e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need.

Supplemental Guidance: Related control: SC-8.

(5) BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION

The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

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.

(6) BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES

[Withdrawn: Incorporated into SC-7 (18)].

(7) BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES

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

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.

(8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers at managed interfaces.

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 (IP) addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Related controls: AC-3, AU-2.

(9) BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC

The information system:

(a) Detects and denies outgoing communications traffic posing a threat to external information systems; and

(b) Audits the identity of internal users associated with denied communications.

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.

(10) BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION

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.

(11) BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC

The information system only allows incoming communications from [*Assignment: organization-defined authorized sources*] routed to [*Assignment: organization-defined authorized destinations*].

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.

(12) BOUNDARY PROTECTION | HOST-BASED PROTECTION

The organization implements [*Assignment: organization-defined host-based boundary protection mechanisms*] at [*Assignment: organization-defined information system components*].

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.

(13) BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS

The organization isolates [*at a minimum, vulnerability scanning tools, audit log servers, patch servers, and CND tools*] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

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.

(14) BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS

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.

(15) BOUNDARY PROTECTION | ROUTE PRIVILEGED NETWORK ACCESSES

The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

Supplemental Guidance: Related controls: AC-2, AC-3, AU-2, SI-4.

(16) BOUNDARY PROTECTION | PREVENT DISCOVERY OF COMPONENTS / DEVICES

The information system prevents discovery of specific system components composing a managed interface.

Supplemental Guidance: This control enhancement protects network addresses of information system components that are part of managed interfaces from discovery through common tools and techniques used to identify devices on networks. Network addresses are not available for discovery (e.g., network address not published or entered in domain name systems), requiring prior knowledge for access. Another obfuscation technique is to periodically change network addresses.

(17) BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS

The information system enforces adherence to protocol formats.

Supplemental Guidance: Information system components that enforce protocol formats include, for example, deep packet inspection firewalls and XML gateways. Such system components verify adherence to protocol formats/specifications (e.g., IEEE) at the application layer and identify significant vulnerabilities that cannot be detected by devices operating at the network or transport layers. Related control: SC-4.

(18) BOUNDARY PROTECTION | FAIL SECURE

The information system fails securely in the event of an operational failure of a boundary protection device.

Supplemental Guidance: Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones), information systems do not enter into unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases. Related controls: CP-2, SC-24.

(19) BOUNDARY PROTECTION | BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS

The information system blocks both inbound and outbound communications traffic between [*Assignment: organization-defined communication clients*] that are independently configured by end users and external service providers.

Supplemental Guidance: Communication clients independently configured by end users and external service providers include, for example, instant messaging clients. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.

(20) BOUNDARY PROTECTION | DYNAMIC ISOLATION / SEGREGATION

The information system provides the capability to dynamically isolate/segregate [*Assignment: organization-defined information system components*] from other components of the system.

Supplemental Guidance: The capability to dynamically isolate or segregate certain internal components of organizational information systems is useful when it is necessary to partition or separate certain components of dubious origin from those components possessing greater trustworthiness. Component isolation reduces the attack surface of organizational information systems. Isolation of selected information system components is also a means of limiting the damage from successful cyber attacks when those attacks occur.

(21) BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS

The organization employs boundary protection mechanisms to separate [*Assignment: organization-defined information system components*] supporting [*Assignment: organization-defined missions and/or business functions*].

Supplemental Guidance: Organizations can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or subnetworks, cross-domain devices separating subnetworks, virtualization techniques, and encrypting information flows among system components using distinct encryption keys. Related controls: CA-9, SC-3.

(22) BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS

The information system implements separate network addresses (i.e., different subnets) to connect to systems in different security domains.

Supplemental Guidance: Decomposition of information systems into subnets helps to provide the appropriate level of protection for network connections to different security domains containing information with different security categories or classification levels.

(23) BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE

The information system disables feedback to senders on protocol format validation failure.

Supplemental Guidance: Disabling feedback to senders when there is a failure in protocol validation format prevents adversaries from obtaining information which would otherwise be unavailable.

References: FIPS Publication 199; NIST Special Publications 800-41, 800-77.

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control: The information system protects the **confidentiality and integrity** of transmitted information.

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.

Data traversing a network at a lower classification level shall be protected using NSA Type-1 encryption. See DoDI 8523.01, *Communications Security (COMSEC)*, for additional information regarding the protection of information during transmission.

When more than one computer network exists within a SAPF, 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:

- Purchasing/making cables with the proper color.
- Placing colored tape every five feet along the cable length.
- Wrapping tape around the length of the cable run.

Table 3-3 provides a standard color scheme for typical non-SAP networks and shall not be used for SAP networks without AO or PSO approval. Additionally, cables processing information at the same classification level shall be bundled together in an orderly manner. All cabling must meet TEMPEST requirements.

Classification/Compartment/ Handling Caveat	**Color**
TS//SCI	Yellow
TS//US Only	Orange
S//US Only	Red
U//FOUO	Green

Table 3-4: Network Cable Color Coding Scheme

When networks are present other than those listed in Table 3-3, a different color must be selected for the network cables to assist in minimizing the risk to classified information systems. This includes SAP networks, even though they are associated with a specific classification level. Colors chosen should be in sharp contrast to colors already in use to easily ascertain the associated network in low light areas/conditions. The following systems/networks are examples of such situations where a different color, other than those specified in Table 3-3, must be selected:

- TS//SCI//SAR
- TS//SAR
- S//SAR
- Coalition/Releasable networks

Reference PE-19 for Information Leakage.

Control Enhancements:

(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION

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 IAW the sensitivity of the information or within a Protected Distribution System (PDS) when traversing areas not approved for the sensitivity of the 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.

Transmission confidentiality applies not only to classified information, but to sensitive unclassified as well. This includes, but is not limited to, such information as PII, HVSACO, CUI, and FOUO. A protected distribution system (PDS) provides physical protection for communications lines and can also provide need-to-know isolation. A PDS must be used to transmit unencrypted classified information through an area of lesser classification or control. For additional information, and where NIST referenced

National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 7003, see CNSSI 7003, *Protective Distribution Systems*.

(2) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE / POST TRANSMISSION HANDLING

The information system maintains the [*Selection (one or more): confidentiality; 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.

(3) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS

The information system implements cryptographic mechanisms to protect message externals unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

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) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL / RANDOMIZE COMMUNICATIONS

The information system implements cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

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.

SC-9 TRANSMISSION CONFIDENTIALITY

[Withdrawn: Incorporated into SC-8].

SC-10 NETWORK DISCONNECT

Control: The information system terminates the network connection associated with a communications session at the end of the session or after **no more than one (1) 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.

SC-11 TRUSTED PATH

Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication*].

Supplemental Guidance: Trusted paths are mechanisms by which users (through input devices) can communicate directly with security functions of information systems with the requisite assurance to support information security policies. The mechanisms can be activated only by users or the security functions of organizational information systems. User responses via trusted paths are protected from modifications by or disclosure to untrusted applications. Organizations employ trusted paths for high-assurance connections between security functions of information systems and users (e.g., during system logons). Enforcement of trusted communications paths is typically provided via an implementation that meets the reference monitor concept. Related controls: AC-16, AC-25.

Control Enhancements:

(1) TRUSTED PATH | LOGICAL ISOLATION

The information system provides a trusted communications path that is logically isolated and distinguishable from other paths.

References: None.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system 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:

(1) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).

(2) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS

The organization produces, controls, and distributes symmetric cryptographic keys using [*Selection: NIST FIPS-compliant; NSA-approved*] key management technology and processes.

(3) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS

The organization produces, controls, and distributes asymmetric cryptographic keys using [*Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key*].

(4) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES

[Withdrawn: Incorporated into SC-12].

(5) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS

[Withdrawn: Incorporated into SC-12].

References: NIST Special Publications 800-56, 800-57.

SC-13 CRYPTOGRAPHIC PROTECTION

Control: The information system implements **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.

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.

> NIST FIPS-compliant cryptography shall be used to protect controlled unclassified information (CUI). To protect classified information and U//HVSACO, see SC-8 for transmission and SC-28 for information at rest.
>
> 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.

Control Enhancements: None.

(1) CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY
[Withdrawn: Incorporated into SC-13].

(2) CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY
[Withdrawn: Incorporated into SC-13].

(3) CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS
[Withdrawn: Incorporated into SC-13].

(4) CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES
[Withdrawn: Incorporated into SC-13].

References: FIPS Publication 140; NIST Special Publication 800-171; Web: http://csrc.nist.gov/cryptval, http://www.cnss.gov.

SC-14 PUBLIC ACCESS PROTECTIONS

[Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].

SC-15 COLLABORATIVE COMPUTING DEVICES

Control: The information system:

a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; 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.

Collaborative computing devices include, but are not limited to, VTC, VoIP telephones, VVoIP, networked white boards, video cameras, and microphones. All collaborative computing devices must be approved by the AO prior to purchase. In addition, all collaborative computing equipment, whether connected to SAP, collateral, or unclassified information systems or networks located in SAPFs must be approved by the PSO prior to introduction into the facility. Collaborative computing devices connecting to unclassified information systems within SAPFs are not recommended.

Any multi-classification collaborative computing devices, VTC or like systems that have video and/or audio capability integrated into one system must be previously evaluated by the appropriate Service SAP CTTA.

Collaborative Computing Device Use

The following requirements apply to the use of all collaborative computing devices, regardless of whether they are used on SCI, SAP, collateral classified, or unclassified networks or systems.

- Collaborative computing devices shall not be remotely activated –no exceptions, nor may they invoke auto-answer capabilities that automatically activate the video and audio recording/transmitting devices. [SC-15.a] Activation of collaborative computing devices requires an explicit action by the user (e.g., in the case of a VTC, the user is required to explicitly turn on the camera, speaker, and microphone) and an explicit indication that the equipment is in use and active. [SC-15.b] Remote activation of a camera or microphone is prohibited, i.e., the auto-answer feature shall be disabled.
- Collaborative computing devices that provide video and/or audio conference capabilities shall provide a clearly visible indication that the video and audio mechanisms are operating to alert personnel in the facility when a collaborative computing session is in progress.
- Camera lenses shall be covered with an opaque covering when the camera is not in use. No systems, documents, or media of higher classification may be displayed or in view of the camera.
- Microphones must have a mute or hold capability (e.g., on/off switch) and should have a push-to-talk button (implemented in hardware or software) when the sensitivity of the collaborative session and environments can differ.
- While conducting a collaborative computing session, users shall take all reasonable measures to ensure that no unintended information is made audible or visible via the collaborative computing device. Users shall advise all personnel in the immediate area that the collaborative computing device will be operating and shall sanitize all sensitive material/systems that may be in view of the collaborative computing device.
- Users shall not leave the collaborative computing device unattended while a session is in progress. Once the collaborative session is completed, the user shall take explicit action to disconnect/terminate the collaborative computing device.

In addition to the above, the following additional requirements apply to all collaborative computing devices used on collateral classified or unclassified networks or systems:

- Desktop level collaborative computing devices may use external loud speakers/amplified sound only if they are installed within a closed room with walls that meet the requirement of the PSO, otherwise a headset must be used.

- Microphones must be used in such a way to ensure no unintended conversations are picked up and transmitted outside the facility. This may be accomplished by using microphones in enclosed offices, or by ensuring no other higher classified discussions occur in the area when the microphone is in use.
- Personnel within the facility shall be notified when a camera or microphone is in use.

Control Enhancements:

(1) COLLABORATIVE COMPUTING DEVICES | PHYSICAL DISCONNECT

The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

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

(2) COLLABORATIVE COMPUTING DEVICES | BLOCKING INBOUND / OUTBOUND COMMUNICATIONS TRAFFIC

[Withdrawn: Incorporated into SC-7].

(3) COLLABORATIVE COMPUTING DEVICES | DISABLING / REMOVAL IN SECURE WORK AREAS

The organization disables or removes collaborative computing devices from [*Assignment: organization-defined information systems or information system components*] in [*Assignment: organization-defined 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) COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS

The information system provides an explicit indication of current participants in [*Assignment: organization-defined online meetings and teleconferences*].

Supplemental Guidance: This control enhancement helps to prevent unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.

References: None.

SC-16 TRANSMISSION OF SECURITY ATTRIBUTES

Control: The information system associates [Assignment: organization-defined security attributes] with information exchanged between information systems and between system components.

Supplemental Guidance: Security attributes can be explicitly or implicitly associated with the information contained in organizational information systems or system components. Related controls: AC-3, AC-4, AC-16.

Control Enhancements:

(1) TRANSMISSION OF SECURITY ATTRIBUTES | INTEGRITY VALIDATION

The information system validates the integrity of transmitted security attributes.

Supplemental Guidance: This control enhancement ensures that the verification of the integrity of transmitted information includes security attributes. Related controls: AU-10, SC-8.

References: None.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.

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.

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 is software obtained from remote systems outside the system authorization boundary, transferred across a network, and then downloaded and executed on a local system (e.g., a computer with a web browser) without explicit installation or execution by the recipient. ‘Transferred across a network’ includes transfers via media, aka sneakernet.

SC-18 is addressed at the highest level by indicating the use or prohibition of mobile code. Mobile code is frequently used even on isolated LANs by the software used to manage systems, e.g., ePolicy orchestrator (the HBSS management tool) uses JAVA for loading its management console; other software may use .Net Framework. sdf

The risks to closed restricted networks and isolated LANs are vastly different than the Global Information Grid (GIG) therefore the mitigations required to address (b) and (c) statements of the control as well as the enhancements should be vastly easier to outline and enumerate.

Potential options for indicating how this control is implemented may include one of the following examples:

- The following are the acceptable uses of mobile code within the system:
  (List known web services on the system that utilize mobile code)
  HBSS Management website: Java.
- The HBSS Management console is DAC’d to sysadmin/IA users only.
- Requests for new mobile code is restricted and must be approved IAW the software approval process (Other than new development this is the most likely way to introduce new mobile code to an isolated network. On systems where mobile code or other software is being developed, typically there is a software approval process that discusses how development is done on the system and how integrity of code and subsequent code libraries is verified.)

Mobile code technologies are software technologies that provide the mechanisms for the production and use of mobile code. Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, PDF, .NET, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Policy and procedures related to mobile code address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system.

DoD SAP policies define three risk categories for mobile code. Following a thorough risk assessment, each mobile code technology is assigned to one of three risk categories:

- **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 DoD SAP operations, and the high risk associated with their use outweighs almost all possible benefits.
- **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 DoD SAP information systems; when combined with prudent countermeasures against malicious code and exploitation, their use can afford benefits that generally outweigh the risks.
- **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 DoD SAP 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.

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]:

- 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.
- 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.
- 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 certificate.
- Category 3 mobile code may be used.

Control Enhancements:

(1) MOBILE CODE | IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS

The information system identifies [*Assignment: organization-defined unacceptable mobile code*] and takes [*Assignment: organization-defined corrective actions*].

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.

(2) MOBILE CODE | ACQUISITION / DEVELOPMENT / USE

The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets [*Assignment: organization-defined mobile code requirements*].

(3) MOBILE CODE | PREVENT DOWNLOADING / EXECUTION

The information system prevents the download and execution of [*Assignment: organization-defined unacceptable mobile code*].

(4) MOBILE CODE | PREVENT AUTOMATIC EXECUTION

The information system prevents the automatic execution of mobile code in [*Assignment: organization-defined software applications*] and enforces [*Assignment: organization-defined actions*] 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 Compact Disks (CDs), Digital Video Disks (DVDs), and Universal Serial Bus (USB) devices.

(5) MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS

The organization allows execution of permitted mobile code only in confined virtual machine environments.

References: NIST Special Publication 800-28; DoD Instruction 8552.01.

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization:

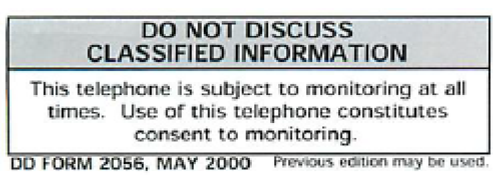
a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of VoIP within the information system.

Supplemental Guidance: Related controls: CM-6, SC-7, SC-15.

Organizations shall ensure VoIP technologies are implemented with AO and PSO approval. Additional guidance is available in the DISA *Voice and Video Over IP (VVoIP) STIG*. In addition, the following shall apply:

- VoIP telephone instruments shall have a "Consent to Monitor" label (e.g., DD Form 2056) or banner and an appropriate classification label or banner. Example of unclassified label below:


DO NOT DISCUSS
CLASSIFIED INFORMATION

This telephone is subject to monitoring at all times. Use of this telephone constitutes consent to monitoring.

DD FORM 2056, MAY 2000 Previous edition may be used.

Figure 3-3: 'Consent to Monitor' Label

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.

Control Enhancements: None.

References: NIST Special Publication 800-58.

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system:

a. Provides additional data origin authentication and integrity verification 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, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. Related controls: 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.

Control Enhancements:

(1) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES

[Withdrawn: Incorporated into SC-20].

(2) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN / INTEGRITY

The information system provides data origin and integrity protection artifacts for internal name/address resolution queries.

References: OMB Memorandum 08-23; NIST Special Publication 800-81.

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.

Control Enhancements: None.

(1) SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | DATA ORIGIN / INTEGRITY

[Withdrawn: Incorporated into SC-21].

References: NIST Special Publication 800-81.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

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

Supplemental Guidance: Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists). Related controls: SC-2, SC-20, SC-21, SC-24.

Control Enhancements: None.

References: NIST Special Publication 800-81.

SC-23 SESSION AUTHENTICITY

Control: The information system protects the authenticity of communications 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:

(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.

(2) SESSION AUTHENTICITY | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS

[Withdrawn: Incorporated into AC-12 (1)].

(3) SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION

The information system generates a unique session identifier for each session with [Assignment: no readily reproducible or 'spoofable' session identifiers] 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) SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION

[Withdrawn: Incorporated into SC-23 (3)].

(5) SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES

The information system only allows the use of [*Assignment: organization-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 Transport Layer Security (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.

SC-24 FAIL IN KNOWN STATE

Control: The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.

Supplemental Guidance: Failure in a known state addresses security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of organizational information systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes. Related controls: CP-2, CP-10, CP-12, SC-7, SC-22.

Control Enhancements: None.

References: None.

SC-25 THIN NODES

Control: The organization employs [*Assignment: organization-defined information system components*] with minimal functionality and information storage.

Supplemental Guidance: The deployment of information system components with reduced/minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to cyber attacks. Related control: SC-30.

Control Enhancements: None.

References: None.

SC-26 HONEYPOTS

Control: The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

Supplemental Guidance: A honeypot is set up as a decoy to attract adversaries and to deflect their attacks away from the operational systems supporting organizational missions/business function. Depending upon the specific usage of the honeypot, consultation with the Office of the General Counsel before deployment may be needed. Related controls: SC-30, SC-44, SI-3, SI-4.

Control Enhancements: None.

(1) HONEYPOTS | DETECTION OF MALICIOUS CODE
[Withdrawn: Incorporated into SC-35].

References: None.

SC-27 PLATFORM-INDEPENDENT APPLICATIONS

Control: The information system includes: [Assignment: organization-defined platform-independent applications].

Supplemental Guidance: Platforms are combinations of hardware and software used to run software applications. Platforms include: (i) operating systems; (ii) the underlying computer architectures, or (iii) both. Platform-independent applications are applications that run on multiple platforms. Such applications promote portability and reconstitution on different platforms, increasing the availability of critical functions within organizations while information systems with specific operating systems are under attack. Related control: SC-29.

Control Enhancements: None.

References: None.

SC-28 PROTECTION OF INFORMATION AT REST

Control: The information system protects the **confidentiality and integrity** of **all SAP 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.

Encryption shall be implemented to complement protection of information at rest, using approved cryptographic methods identified in SC-13. Reference [MP-5] for data encryption as well as media transport requirements, i.e., mobile devices and removable media.

Information at rest refers to the state of information when it is located on a non-volatile device (e.g., hard drive, tapes, optical discs, flash drives). This also includes workstations, servers, and off-line storage.

This control is non-tailorable for all SAP systems.

Control Enhancements:

(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*Assignment: organization-defined information system components*].

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)].

(2) PROTECTION OF INFORMATION AT REST | OFF-LINE STORAGE

The organization removes from online storage and stores off-line in a secure location [*Assignment: organization-defined information*].

Supplemental Guidance: Removing organizational information from online information system storage to off-line storage eliminates the possibility of individuals gaining unauthorized access to the information through a network. Therefore, organizations may choose to move information to off-line storage in lieu of protecting such information in online storage.

References: NIST Special Publications 800-56, 800-57, 800-111.

SC-29 HETEROGENEITY

Control: The organization employs a diverse set of information technologies for [*Assignment: organization-defined information system components*] in the implementation of the information system.

Supplemental Guidance: Increasing the diversity of information technologies within organizational information systems reduces the impact of potential exploitations of specific technologies and also defends against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one information system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned cyber attacks. An increase in diversity may add complexity and management overhead which could ultimately lead to mistakes and unauthorized configurations. Related controls: SA-12, SA-14, SC-27.

Control Enhancements:

(1) HETEROGENEITY | VIRTUALIZATION TECHNIQUES

The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [*Assignment: organization-defined frequency*].

Supplemental Guidance: While frequent changes to operating systems and applications pose configuration management challenges, the changes can result in an increased work factor for adversaries in order to carry out successful cyber attacks. Changing virtual operating systems or applications, as opposed to changing actual operating systems/applications, provide virtual changes that impede attacker success while reducing configuration management efforts. In addition, virtualization techniques can assist organizations in isolating untrustworthy software and/or software of dubious provenance into confined execution environments.

References: None.

SC-30 CONCEALMENT AND MISDIRECTION

Control: The organization employs [*Assignment: organization-defined concealment and misdirection techniques*] for [*Assignment: organization-defined information systems*] at [*Assignment: organization-defined time periods*] to confuse and mislead adversaries.

Supplemental Guidance: Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber attacks. For example, virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Increased use of concealment/misdirection techniques including, for example, randomness, uncertainty, and virtualization, may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment/misdirection techniques may also provide organizations additional time to successfully perform core missions and business functions. Because of the time and effort required to support concealment/misdirection techniques, it is anticipated that such techniques would be used by organizations on a very limited basis. Related controls: SC-26, SC-29, SI-14.

Control Enhancements:

(1) CONCEALMENT AND MISDIRECTION | VIRTUALIZATION TECHNIQUES

[Withdrawn: Incorporated into SC-29 (1)].

(2) CONCEALMENT AND MISDIRECTION | RANDOMNESS

The organization employs [*Assignment: organization-defined techniques*] to introduce randomness into organizational operations and assets.

Supplemental Guidance: Randomness introduces increased levels of uncertainty for adversaries regarding the actions organizations take in defending against cyber attacks. Such actions may impede the ability of adversaries to correctly target information resources of organizations supporting critical missions/business functions. Uncertainty may also cause adversaries to hesitate before initiating or continuing attacks. Misdirection techniques involving randomness include, for example, performing certain routine actions at different times of day, employing different information technologies (e.g., browsers, search engines), using different suppliers, and rotating roles and responsibilities of organizational personnel.

(3) CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING / STORAGE LOCATIONS

The organization changes the location of [*Assignment: organization-defined processing and/or storage*] [*Selection: [Assignment: organization-defined time frequency]; at random time intervals*]].

Supplemental Guidance: Adversaries target critical organizational missions/business functions and the information resources supporting those missions and functions while at the same time, trying to minimize exposure of their existence and tradecraft. The static, homogeneous, and deterministic nature of organizational information systems targeted by adversaries, make such systems more susceptible to cyber attacks with less adversary cost and effort to be successful. Changing organizational processing and storage locations (sometimes referred to as moving target defense) addresses the advanced persistent threat (APT) using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the information resources (i.e., processing and/or storage) supporting critical missions and business functions. Changing locations of processing activities and/or storage sites introduces uncertainty into the targeting activities by adversaries. This uncertainty increases the work factor of adversaries making compromises or breaches to organizational information systems much more difficult and time-consuming, and increases the chances that adversaries may inadvertently disclose aspects of tradecraft while attempting to locate critical organizational resources.

(4) CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION

The organization employs realistic, but misleading information in [*Assignment: organization-defined information system components*] with regard to its security state or posture.

Supplemental Guidance: This control enhancement misleads potential adversaries regarding the nature and extent of security safeguards deployed by organizations. As a result, adversaries may employ incorrect (and as a result ineffective) attack techniques. One way of misleading adversaries is for organizations to place misleading information regarding the specific security controls deployed in external information systems that are known to be accessed or targeted by adversaries. Another technique is the use of deception nets (e.g., honeynets, virtualized environments) that mimic actual aspects of organizational information systems but use, for example, out-of-date software configurations.

(5) CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS

The organization employs [*Assignment: organization-defined techniques*] to hide or conceal [*Assignment: organization-defined information system components*].

Supplemental Guidance: By hiding, disguising, or otherwise concealing critical information system components, organizations may be able to decrease the probability that adversaries target and successfully compromise those assets. Potential means for organizations to hide and/or conceal information system components include, for example, configuration of routers or the use of honeynets or virtualization techniques.

References: None.

SC-31 COVERT CHANNEL ANALYSIS

Control: The organization:

a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [*Selection (one or more): storage; timing*] channels; and

b. Estimates the maximum bandwidth of those channels.

Supplemental Guidance: Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, for example, in the case of information systems containing export-controlled information and having connections to external networks (i.e., networks not controlled by organizations). Covert channel analysis is also meaningful for multilevel secure (MLS) information systems, multiple security level (MSL) systems, and cross-domain systems. Related controls: AC-3, AC-4, PL-2.

Control Enhancements:

(1) COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY

The organization tests a subset of the identified covert channels to determine which channels are exploitable.

(2) COVERT CHANNEL ANALYSIS | MAXIMUM BANDWIDTH

The organization reduces the maximum bandwidth for identified covert [*Selection (one or more); storage; timing*] channels to [*Assignment: organization-defined values*].

Supplemental Guidance: Information system developers are in the best position to reduce the maximum bandwidth for identified covert storage and timing channels.

(3) COVERT CHANNEL ANALYSIS | MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS

The organization measures the bandwidth of [As*signment: organization-defined subset of identified covert channels*] in the operational environment of the information system.

Supplemental Guidance: This control enhancement addresses covert channel bandwidth in operational environments versus developmental environments. Measuring covert channel bandwidth in operational environments helps organizations to determine how much information can be covertly leaked before such leakage adversely affects organizational missions/business functions. Covert channel bandwidth may be significantly different when measured in those settings that are independent of the particular environments of operation (e.g., laboratories or development environments).

References: None.

SC-32 INFORMATION SYSTEM PARTITIONING

Control: The organization partitions the information system into [*Assignment: organization-defined information system components*] residing in separate physical domains or environments based on [*Assignment: organization-defined circumstances for physical separation of components*].

Supplemental Guidance: Information system partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the more critical components, to more significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components. Related controls: AC-4, SA-8, SC-2, SC-3, SC-7.

Control Enhancements: None.

References: FIPS Publication 199.

SC-33 TRANSMISSION PREPARATION INTEGRITY

[Withdrawn: Incorporated into SC-8].

SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS

Control: The information system at [*Assignment: organization-defined information system components*]:

a. Loads and executes the operating environment from hardware-enforced, read-only media; and

b. Loads and executes [*Assignment: organization-defined applications*] from hardware-enforced, read-only media.

Supplemental Guidance: The term operating environment is defined as the specific code that hosts applications, for example, operating systems, executives, or monitors including virtual machine monitors (i.e., hypervisors). It can also include certain applications running directly on hardware platforms. Hardware-enforced, read-only media include, for example, Compact Disk-Recordable (CD-R)/Digital Video Disk-Recordable (DVD-R) disk drives and one-time programmable read-only memory. The use of non-modifiable storage ensures the integrity of software from the point of creation of the read-only image. The use of reprogrammable read-only memory can be accepted as read-only media provided: (i) integrity can be adequately protected from the point of initial writing to the insertion of the memory into the information system; and (ii) there are reliable hardware protections against reprogramming the memory while installed in organizational information systems. Related controls: AC-3, SI-7.

Control Enhancements:

(1) NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE

The organization employs [*Assignment: organization-defined information system components*] with no writeable storage that is persistent across component restart or power on/off.

Supplemental Guidance: This control enhancement: (i) eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated information system components; and (ii) applies to both fixed and removable storage, with the latter being addressed directly or as specific restrictions imposed through access controls for mobile devices. Related controls: AC-19, MP-7.

(2) NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION / READ-ONLY MEDIA

The organization protects the integrity of information prior to storage on read-only media and controls the media after such information has been recorded onto the media.

Supplemental Guidance: Security safeguards prevent the substitution of media into information systems or the reprogramming of programmable read-only media prior to installation into the systems. Security safeguards include, for example, a combination of prevention, detection, and response. Related controls: AC-5, CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SA-12, SC-28, SI-3.

(3) NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION

The organization:

(a) Employs hardware-based, write-protect for [*Assignment: organization-defined information system firmware components*]; and

(b) Implements specific procedures for [*Assignment: organization-defined authorized individuals*] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.

References: None.

SC-35 HONEYCLIENTS

Control: The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.

Supplemental Guidance: Honeyclients differ from honeypots in that the components actively probe the Internet in search of malicious code (e.g., worms) contained on external websites. As with honeypots, honeyclients require some supporting isolation measures (e.g., virtualization) to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational information systems. Related controls: SC-26, SC-44, SI-3, SI-4.

Control Enhancements: None.

References: None.

SC-36 DISTRIBUTED PROCESSING AND STORAGE

Control: The organization distributes [*Assignment: organization-defined processing and storage*] across multiple physical locations.

Supplemental Guidance: Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and thus allows for parallel processing and storage. Related controls: CP-6, CP-7.

Control Enhancements:

(1) DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES

The organization employs polling techniques to identify potential faults, errors, or compromises to [*Assignment: organization-defined distributed processing and storage components*].

Supplemental Guidance: Distributed processing and/or storage may be employed to reduce opportunities for adversaries to successfully compromise the confidentiality, integrity, or availability of information and information systems. However, distribution of processing and/or storage components does not prevent adversaries from compromising one (or more) of the distributed components. Polling compares the processing results and/or storage content from the various distributed components and subsequently voting on the outcomes. Polling identifies potential faults, errors, or compromises in distributed processing and/or storage components. Related control: SI-4.

References: None.

SC-37 OUT-OF-BAND CHANNELS

Control: The organization employs [*Assignment: organization-defined out-of-band channels*] for the physical delivery or electronic transmission of [*Assignment: organization-defined information, information system components, or devices*] to [A*ssignment: organization-defined individuals or information systems*].

Supplemental Guidance: Out-of-band channels include, for example, local (nonnetwork) accesses to information systems, network paths physically separate from network paths used for operational traffic, or nonelectronic paths such as the US Postal Service. This is in contrast with using the same channels (i.e., in-band channels) that carry routine operational traffic. Out-of-band channels do not have the same vulnerability/exposure as in-band channels, and hence the confidentiality, integrity, or availability compromises of in-band channels will not compromise the out-of-band channels. Organizations may employ out-of-band channels in the delivery or transmission of many organizational items including, for example, identifiers/authenticators, configuration management changes for hardware, firmware, or software, cryptographic key management information, security updates, system/data backups, maintenance information, and malicious code protection updates. Related controls: AC-2, CM-3, CM-5, CM-7, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.

Control Enhancements:

(1) OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION

The organization employs [*Assignment: organization-defined security safeguards*] to ensure that only [*Assignment: organization-defined individuals or information systems*] receive the [*Assignment: organization-defined information, information system components, or devices*].

Supplemental Guidance: Techniques and/or methods employed by organizations to ensure that only designated information systems or individuals receive particular information, system components, or devices include, for example, sending authenticators via courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.

References: None.

SC-38 OPERATIONS SECURITY

Control: The organization employs [*Assignment: organization-defined operations security 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: (i) identification of critical information (e.g., the security categorization process); (ii) analysis of threats; (iii) analysis of vulnerabilities; (iv) assessment of risks; and (v) 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.

SC-39 PROCESS ISOLATION

Control: The information system 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.

Control Enhancements:

(1) PROCESS ISOLATION | HARDWARE SEPARATION

The information system implements underlying hardware separation mechanisms to facilitate process separation.

Supplemental Guidance: Hardware-based separation of information system processes is generally less susceptible to compromise than software-based separation, thus providing greater assurance that the separation will be enforced. Underlying hardware separation mechanisms include, for example, hardware memory management.

(2) PROCESS ISOLATION | THREAD ISOLATION

The information system maintains a separate execution domain for each thread in [*Assignment: organization-defined multi-threaded processing*].

References: None.

SC-40 WIRELESS LINK PROTECTION

Control: The information system protects external and internal [*Assignment: organization-defined wireless links*] from [*Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks*].

Supplemental Guidance: This control applies to internal and external wireless communication links that may be visible to individuals who are not authorized information system users. Adversaries can exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or to spoof users of organizational information systems. This control reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may not be possible to implement this control. Related controls: AC-18, SC-5.

Control Enhancements:

(1) WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE

The information system implements cryptographic mechanisms that achieve [*Assignment: organization-defined level of protection*] against the effects of intentional electromagnetic interference.

Supplemental Guidance: This control enhancement protects against intentional jamming that might deny or impair communications by ensuring that wireless spread spectrum waveforms used to provide anti-jam protection are not predictable by unauthorized individuals. The control enhancement may also coincidentally help to mitigate the effects of unintentional jamming due to interference from legitimate transmitters sharing the same spectrum. Mission requirements, projected threats, concept of operations, and applicable legislation, directives, regulations, policies, standards, and guidelines determine levels of wireless link availability and performance/cryptography needed. Related controls: SC-12, SC-13.

(2) WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL

The information system implements cryptographic mechanisms to reduce the detection potential of wireless links to [*Assignment: organization-defined level of reduction*].

Supplemental Guidance: This control enhancement is needed for covert communications and protecting wireless transmitters from being geo-located by their transmissions. The control enhancement ensures that spread spectrum waveforms used to achieve low probability of detection are not predictable by unauthorized individuals. Mission requirements, projected threats, concept of operations, and applicable legislation, directives, regulations, policies, standards, and guidelines determine the levels to which wireless links should be undetectable. Related controls: SC-12, SC-13.

(3) WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION

The information system implements cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.

Supplemental Guidance: This control enhancement ensures that the signal parameters of wireless transmissions are not predictable by unauthorized individuals. Such unpredictability reduces the probability of imitative or manipulative communications deception based upon signal parameters alone. Related controls: SC-12, SC-13.

(4) WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION

The information system implements cryptographic mechanisms to prevent the identification of [Assignment: organization-defined wireless transmitters] by using the transmitter signal parameters.

Supplemental Guidance: Radio fingerprinting techniques identify the unique signal parameters of transmitters to fingerprint such transmitters for purposes of tracking and mission/user identification. This control enhancement protects against the unique identification of wireless transmitters for purposes of intelligence exploitation by ensuring that anti-fingerprinting alterations to signal parameters are not predictable by unauthorized individuals. This control enhancement helps assure mission success when anonymity is required. Related controls: SC-12, SC-13.

References: None.

SC-41 PORT AND I/O DEVICE ACCESS

Control: The organization physically disables or removes [*Assignment: organization-defined connection ports or input/output devices*] on [*Assignment: organization-defined information systems or information system components*].

Supplemental Guidance: Connection ports include, for example, Universal Serial Bus (USB) and Firewire (IEEE 1394). Input/output (I/O) devices include, for example, Compact Disk (CD) and Digital Video Disk (DVD) drives. Physically disabling or removing such connection ports and I/O devices helps prevent exfiltration of information from information systems and the introduction of malicious code into systems from those ports/devices.

Control Enhancements: None.

References: None.

SC-42 SENSOR CAPABILITY AND DATA

Control: The information system:

a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [*Assignment: organization-defined exceptions where remote activation of sensors is allowed*]; and

b. Provides an explicit indication of sensor use to [*Assignment: organization-defined class of users*].

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, Global Positioning System (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:

(1) SENSOR CAPABILITY AND DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES

The organization ensures that the information system is configured so that data or information collected by the [*Assignment: organization-defined sensors*] is only reported to authorized individuals or roles.

Supplemental Guidance: In situations where sensors are activated by authorized individuals (e.g., end users), it is still possible that the data/information collected by the sensors will be sent to unauthorized entities.

(2) SENSOR CAPABILITY AND DATA | AUTHORIZED USE

The organization employs the following measures: [*Assignment: organization-defined measures*], so that data or information collected by [*Assignment: organization-defined sensors*] is only used for authorized purposes.

Supplemental Guidance: Information collected by sensors for a specific authorized purpose potentially could be misused for some unauthorized purpose. For example, GPS sensors that are used to support traffic navigation could be misused to track movements of individuals. Measures to mitigate such activities include, for example, additional training to ensure that authorized parties do not abuse their authority, or (in the case where sensor data/information is maintained by external parties) contractual restrictions on the use of the data/information.

(3) SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES

The organization prohibits the use of devices possessing [*Assignment: organization-defined environmental sensing capabilities*] in [*Assignment: organization-defined facilities, areas, or systems*].

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.

SC-43 USAGE RESTRICTIONS

Control: The organization:

a. Establishes usage restrictions and implementation guidance for [*Assignment: organization-defined information system components*] based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of such components within the information system.

Supplemental Guidance: Information system components include hardware, software, or firmware components (e.g., Voice Over Internet Protocol, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices). Related controls: CM-6, SC-7.

<u>Control Enhancements</u>: None.

<u>References</u>: None.

SC-44 DETONATION CHAMBERS

<u>Control</u>: The organization employs a detonation chamber capability within [*Assignment: organization-defined information system, system component, or location*].

<u>Supplemental Guidance</u>: Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox. These protected and isolated execution environments provide a means of determining whether the associated attachments/applications contain malicious code. While related to the concept of deception nets, the control is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, it is intended to quickly identify malicious code and reduce the likelihood that the code is propagated to user environments of operation (or prevent such propagation completely). Related controls: SC-7, SC-25, SC-26, SC-30.

<u>Control Enhancements</u>: None.

<u>References</u>: None.

FAMILY: SYSTEM AND INFORMATION INTEGRITY

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.

DoD SAP-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.

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.

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 Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature 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.

> 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:
>
> - 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.
> - Employ automated patch management tools on all components to the maximum extent supported by available tools to facilitate flaw remediation.
>
> PM-14 is another related control.

Control Enhancements:

(1) FLAW REMEDIATION | CENTRAL MANAGEMENT

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.

(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

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.

(3) FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS

The organization:

(a) Measures the time between flaw identification and flaw remediation; and

(b) Establishes [*Assignment: organization-defined benchmarks*] for taking corrective actions.

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) FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS

[Withdrawn: Incorporated into SI-2].

(5) FLAW REMEDIATION | AUTOMATIC SOFTWARE / FIRMWARE UPDATES

The organization installs [*Assignment: organization-defined security-relevant software and firmware updates*] automatically to [*Assignment: organization-defined information system components*].

Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Organizations must balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and with any mission or operational impacts that automatic updates might impose.

(6) FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE

The organization removes [*Assignment: organization-defined software and 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.

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 then send an alert to the system administrator**; [*Assignment: organization-defined action*]] in response to malicious code detection; and

d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

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:

(1) MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT

The organization centrally manages malicious code protection mechanisms.

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.

(2) MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES

The information system automatically updates malicious code protection mechanisms.

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.

(3) MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS

[Withdrawn: Incorporated into AC-6 (10)].

(4) MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED USERS

The information system updates malicious code protection mechanisms only when directed by a privileged user.

Supplemental Guidance: This control enhancement may be appropriate for situations where for reasons of security or operational continuity, updates are only applied when selected/approved by designated organizational personnel. Related controls: AC-6, CM-5.

(5) MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES

[Withdrawn: Incorporated into MP-7].

(6) MALICIOUS CODE PROTECTION | TESTING / VERIFICATION

The organization:

(a) Tests malicious code protection mechanisms [*Assignment: organization-defined frequency*] by introducing a known benign, non-spreading test case into the information system; and

(b) Verifies that both detection of the test case and associated incident reporting occur.

Supplemental Guidance: Related controls: CA-2, CA-7, RA-5.

(7) MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION

The information system implements nonsignature-based malicious code detection mechanisms.

Supplemental Guidance: Nonsignature-based detection mechanisms include, for example, the use of heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective. This includes polymorphic malicious code (i.e., code that changes signatures when it replicates). This control enhancement does not preclude the use of signature-based detection mechanisms.

(8) MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS

The information system detects [*Assignment: organization-defined unauthorized operating system commands*] through the kernel application programming interface at [*Assignment: organization-defined information system hardware components*] and **audits the command execution and prevents the execution of the command**.

Supplemental Guidance: This control enhancement can also be applied to critical interfaces other than kernel-based interfaces, including for example, interfaces with virtual machines and privileged applications. Unauthorized operating system commands include, for example, commands for kernel functions from information system processes that are not trusted to initiate such commands, or commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate. Organizations can define the malicious commands to be detected by a combination of command types, command classes, or specific instances of commands. Organizations can define hardware components by specific component, component type, location in the network, or combination therein. Organizations may select different actions for different types/classes/specific instances of potentially malicious commands. Related control: AU-6.

(9) MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS

The information system implements [*Assignment: organization-defined security safeguards*] to authenticate [*Assignment: organization-defined remote commands*].

Supplemental Guidance: This control enhancement protects against unauthorized commands and replay of authorized commands. This capability is important for those remote information systems whose loss, malfunction, misdirection, or exploitation would have immediate and/or serious consequences (e.g., injury or death, property damage, loss of high-valued assets or sensitive information, or failure of important missions/business functions). Authentication safeguards for remote commands help to ensure that information systems accept and execute in the order intended, only authorized commands, and that unauthorized commands are rejected. Cryptographic mechanisms can be employed, for example, to authenticate remote commands. Related controls: SC-12, SC-13, SC-23.

(10) MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS

The organization:

(a) Employs [*Assignment: organization-defined 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 tradecraft (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.

Malicious code analysis is frequently conducted by a trained forensics team.

References: NIST Special Publication 800-83.

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 [*Assignment: organization-defined monitoring objectives*]; and

2. Unauthorized local, network, and remote connections;

b. Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];

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 [*Assignment: organization-defined information system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed*; [*Assignment: organization-defined frequency*]].

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:

(1) INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

(2) INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS

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.

(3) INFORMATION SYSTEM MONITORING | AUTOMATED TOOL INTEGRATION

The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

(4) INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

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.

(5) INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS

The information system alerts Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].

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.

(6) INFORMATION SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS

[Withdrawn: Incorporated into AC-6 (10)].

(7) INFORMATION SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS

The information system notifies [*Assignment: organization-defined incident response personnel (identified by name and/or by role)*] of detected suspicious events and takes [*Assignment: organization-defined least-disruptive actions to terminate suspicious events*].

Supplemental Guidance: Least-disruptive actions may include, for example, initiating requests for human responses.

> The least disruptive action is appropriately determined for each individual system. Notification may equate to an email notification to a system administrator, who must then contact incident response personnel within their command chain.

(8) INFORMATION SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION

[Withdrawn: Incorporated into SI-4].

(9) INFORMATION SYSTEM MONITORING | TESTING OF MONITORING TOOLS

The organization tests intrusion-monitoring tools **at least monthly.**

Supplemental Guidance: Testing intrusion-monitoring tools is necessary to ensure that the tools are operating correctly and continue to meet the monitoring objectives of organizations. The frequency of testing depends on the types of tools used by organizations and methods of deployment. Related control: CP-9.

(10) INFORMATION SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS

The organization makes provisions so that [*Assignment: organization-defined encrypted communications traffic*] is visible to [*Assignment: organization-defined information system 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.

(11) INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES

The organization analyzes outbound communications traffic at the external boundary of the information system and selected [*Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)*] to discover anomalies.

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.

(12) INFORMATION SYSTEM MONITORING | AUTOMATED ALERTS

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**.

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.

Organizations will list alerts that their monitoring software is configured to provide. 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.

(13) INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS

The organization:

(a) Analyzes communications traffic/event patterns for the information system;

(b) Develops profiles representing common traffic patterns and/or events; and

(c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.

(14) INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION

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.

(15) INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS

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.

(16) INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION

The organization correlates information from monitoring tools employed throughout the information system.

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.

(17) INFORMATION SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS

The organization correlates information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.

Supplemental Guidance: This control enhancement correlates monitoring information from a more diverse set of information sources to achieve integrated situational awareness. Integrated situational awareness from a combination of physical, cyber, and supply chain monitoring activities enhances the capability of organizations to more quickly detect sophisticated cyber attacks and investigate the methods and techniques employed to carry out such attacks. In contrast to SI-4 (16) which correlates the various cyber monitoring information, this control enhancement correlates monitoring beyond just the cyber domain. Such monitoring may help reveal attacks on organizations that are operating across multiple attack vectors. Related control: SA-12.

(18) INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / COVERT EXFILTRATION

The organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at [*Assignment: organization-defined interior points within the system (e.g., subsystems, subnetworks)*] to detect covert exfiltration of information.

Supplemental Guidance: Covert means that can be used for the unauthorized exfiltration of organizational information include, for example, steganography.

(19) INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK

The organization implements [*Assignment: organization-defined additional monitoring*] of individuals who have been identified by [*Assignment: organization-defined sources*] as posing an increased level of risk.

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.

(20) INFORMATION SYSTEM MONITORING | PRIVILEGED USER

The organization implements [*Assignment: organization-defined additional monitoring*] of privileged users.

> Implementation of AU-2 controls may address this security control. Identify additional monitoring activities required by the AO.

(21) INFORMATION SYSTEM MONITORING | PROBATIONARY PERIODS

The organization implements [*Assignment: organization-defined additional monitoring*] of individuals during [*Assignment: organization-defined probationary period*].

> 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 PSO/GSSO/CPSO institutes probationary period of 30 days during which time a designated security person reviews all documents produced by the individual.

(22) INFORMATION SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES

The information system detects network services that have not been authorized or approved by [*Assignment: organization-defined authorization or approval processes*] and [*Selection (one or more): audits; alerts [Assignment: organization-defined personnel or roles*]].

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.

(23) INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES

The organization implements [*Assignment: organization-defined host-based monitoring mechanisms*] at [*Assignment: organization-defined information system components*].

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)].

(24) INFORMATION SYSTEM MONITORING | INDICATORS OF COMPROMISE

The information system discovers, collects, distributes, and uses indicators of compromise.

Supplemental Guidance: Indicators of compromise (IOC) are forensic artifacts from intrusions that are identified on organizational information systems (at the host or network level). IOCs provide organizations with valuable information on objects or information systems that have been compromised. IOCs for the discovery of compromised hosts can include for example, the creation of registry key values. IOCs for network traffic include, for example, Universal Resource Locator (URL) or protocol elements that indicate malware command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that information systems and organizations are vulnerable to the same exploit or attack.

References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137.

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, DHS US-CERT, SANS Internet Storm Center (ISC) and USCYBERCOM** on an ongoing basis;

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**; [*Assignment: organization-defined elements within the organization*]; [*Assignment: organization-defined external organizations*]]; 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. The DoD Information Assurance Vulnerability (IAV) Management (IAVM) process was created to develop and disseminate mitigating actions for critical software vulnerabilities to DoD Components. US Cyber Command (USCYBERCOM) and DISA jointly manage the IAVM and Computer Network Directives, and both identify and publish vulnerabilities or directives. IAVM notices have three levels of criticality:

- IAV Alert (IAVA) – most critical – a vulnerability posing an immediate and potentially sever threat to DoD systems.
- IAV Bulletin (IAVB) – less critical than IAVA, but pose a threat to DoD systems.
- IAV Technical Advisory (IAVT) – less critical than IAVB.

IAVAs and IAVBs are maintained by USCYBERCOM and DISA.

Additional sources of alerts and advisories which may be monitored include:

- Department of Homeland Security (DHS) US Computer Emergency Readiness Team (US-CERT).
- Military service computer security incident response teams (CSIRT) (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)).
- Advisories from the IC Security Coordination Center (IC-SCC) such as Intelligence Community Vulnerability Alerts (ICVA) and Intelligence Community Vulnerability Management (ICVM) releases.
- IAVAs and IAVBs maintained by USCYBERCOM and DISA.

Control Enhancements:

(1) SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

Supplemental Guidance: The significant number of changes to organizational information systems and the environments in which those systems operate requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational missions and business functions. Based on the information provided by the security alerts and advisories, changes may be required at one or more of the three tiers related to the management of information security risk including the governance level, mission/business process/enterprise architecture level, and the information system level.

References: NIST Special Publication 800-40.

SI-6 SECURITY FUNCTION VERIFICATION

Control: The information system:

a. Verifies the correct operation of [*Assignment: organization-defined security functions*];

b. Performs this verification [*Assignment: organization-defined system transitional states*];

c. Notifies [*Assignment: organization-defined personnel or roles*] of failed security verification tests; and

d. [*Selection (one or more): shuts the information system down; restarts the information system*; [*Assignment: organization-defined alternative action(s)*]] when anomalies are discovered.

Supplemental Guidance: Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights. Related controls: CA-7, CM-6.

Control Enhancements:

(1) SECURITY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS

[Withdrawn: Incorporated into SI-6].

(2) SECURITY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING

The information system implements automated mechanisms to support for the management of distributed security testing.

Supplemental Guidance: Related control: SI-2.

(3) SECURITY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS

The organization reports the results of security function verification to **responsible security personnel (e.g., PSO, AO, CISO, ISSM/ISSO)**.

Supplemental Guidance: Organizational personnel with potential interest in security function verification results include, for example, senior information security officers, information system security managers, and information systems security officers. Related controls: SA-12, SI-4, SI-5.

References: None.

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Control: The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*].

Supplemental Guidance: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3.

Integrity verification applications shall be employed on information systems to look for evidence of information tampering, errors, and omissions. Good software engineering practices shall be employed with regard to COTS integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes).

Organizations shall employ tracking systems software and associated documentation protected by quantity licenses to control copying and distribution. For smaller systems, a tracking system may be a simple spreadsheet. For more complex systems an automated capability may be required.

Installation of software by users, including privileged users, is prohibited within the DoD SAP Community unless done IAW with the process specifically approved by the AO. Reference approved process outlined in CM-2, CM-2(4), and CM-2(5) and SI-4.

Control Enhancements:

(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS

The information system performs an integrity check of [*Assignment: organization-defined software, firmware, and information*] [*Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events*]; [Assignment: organization-defined frequency].

Supplemental Guidance: Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.

(2) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS

The organization employs automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.

Supplemental Guidance: The use of automated tools to report integrity violations and to notify organizational personnel in a timely matter is an essential precursor to effective risk response. Personnel having an interest in integrity violations include, for example, mission/business owners, information system owners, systems administrators, software developers, systems integrators, and information security officers.

(3) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY-MANAGED INTEGRITY TOOLS

The organization employs centrally managed integrity verification tools.

Supplemental Guidance: Related controls: AU-3, SI-2, SI-8.

(4) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER-EVIDENT PACKAGING

[Withdrawn: Incorporated into SA-12].

(5) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS

The information system automatically [*Selection (one or more): shuts the information system down; restarts the information system; implements* [*Assignment: organization-defined security safeguards*]] when integrity violations are discovered.

Supplemental Guidance: Organizations may define different integrity checking and anomaly responses: (i) by type of information (e.g., firmware, software, user data); (ii) by specific information (e.g., boot firmware, boot firmware for a specific types of machines); or (iii) a combination of both. Automatic implementation of specific safeguards within organizational information systems includes, for example, reversing the changes, halting the information system, or triggering audit alerts when unauthorized modifications to critical security files occur.

(6) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION

The information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

Supplemental Guidance: Cryptographic mechanisms used for the protection of integrity include, for example, digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Related control: SC-13.

(7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE

The organization incorporates the detection of unauthorized [*Assignment: organization-defined security-relevant changes to the information system*] into the organizational incident response capability.

Supplemental Guidance: This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges. Related controls: IR-4, IR-5, SI-4.

(8) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS

The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [*Selection (one or more): generates an audit record; alerts current user; alerts* [*Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined other actions*]].

Supplemental Guidance: Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations. Related controls: AU-2, AU-6, AU-12.

(9) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS

The information system verifies the integrity of the boot process of **all devices capable of verification of the boot process**.

Supplemental Guidance: Ensuring the integrity of boot processes is critical to starting devices in known/trustworthy states. Integrity verification mechanisms provide organizational personnel with assurance that only trusted code is executed during boot processes.

(10) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE

The information system implements [*Assignment: organization-defined security safeguards*] to protect the integrity of boot firmware in [*Assignment: organization-defined devices*].

Supplemental Guidance: Unauthorized modifications to boot firmware may be indicative of a sophisticated, targeted cyber attack. These types of cyber attacks can result in a permanent denial of service (e.g., if the firmware is corrupted) or a persistent malicious code presence (e.g., if code is embedded within the firmware). Devices can protect the integrity of the boot firmware in organizational information systems by: (i) verifying the integrity and authenticity of all updates to the boot firmware prior to applying changes to the boot devices; and (ii) preventing unauthorized processes from modifying the boot firmware.

(11) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES

The organization requires that [*Assignment: organization-defined user-installed software*] execute in a confined physical or virtual machine environment with limited privileges.

Supplemental Guidance: Organizations identify software that may be of greater concern with regard to origin or potential for containing malicious code. For this type of software, user installations occur in confined environments of operation to limit or contain damage from malicious code that may be executed.

(12) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION

The organization requires that the integrity of [*Assignment: organization-defined user-installed software*] be verified prior to execution.

Supplemental Guidance: Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or code that contains errors from unauthorized modifications. Organizations consider the practicality of approaches to verifying software integrity including, for example, availability of checksums of adequate trustworthiness from software developers or vendors.

(13) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS

The organization allows execution of binary or machine-executable code obtained from sources with limited or no warranty and without the provision of source code only in confined physical or virtual machine environments and with the explicit approval of **the Authorizing Official (AO).**

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.

(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.

Consider tailoring out if base control (SI-7) is not implemented.

(15) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION

The information system implements cryptographic mechanisms to authenticate **all software and firmware from vendors/sources that provide cryptographic mechanisms to enable the validation of code authenticity and integrity** prior to installation.

Supplemental Guidance: Cryptographic authentication includes, for example, verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code.

(16) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION W/O SUPERVISION

The organization does not allow processes to execute without supervision for more than [*Assignment: organization-defined time period*].

Supplemental Guidance: This control enhancement addresses processes for which normal execution periods can be determined and situations in which organizations exceed such periods. Supervision includes, for example, operating system timers, automated responses, or manual oversight and response when information system process anomalies occur.

References: NIST Special Publications 800-147, 800-155.

SI-8 SPAM PROTECTION

Control: The organization:

a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and

b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions. Related controls: AT-2, AT-3, SC-5, SC-7, SI-3.

Control Enhancements:

(1) SPAM PROTECTION | CENTRAL MANAGEMENT

The organization centrally manages spam protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls. Related controls: AU-3, SI-2, SI-7.

(2) SPAM PROTECTION | AUTOMATIC UPDATES

The information system automatically updates spam protection mechanisms.

(3) SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY

The information system implements spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.

Supplemental Guidance: Learning mechanisms include, for example, Bayesian filters that respond to user inputs identifying specific traffic as spam or legitimate by updating algorithm parameters and thereby more accurately separating types of traffic.

References: NIST Special Publication 800-45.

SI-9 INFORMATION INPUT RESTRICTIONS

[Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-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.

Control Enhancements:

(1) INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY

The information system:

(a) Provides a manual override capability for input validation of [*Assignment: organization-defined inputs*];

(b) Restricts the use of the manual override capability to only [*Assignment: organization-defined authorized individuals*]; and

(c) Audits the use of the manual override capability.

Supplemental Guidance: Related controls: CM-3, CM-5.

(2) INFORMATION INPUT VALIDATION | REVIEW / RESOLUTION OF ERRORS

The organization ensures that input validation errors are reviewed and resolved within [*Assignment: organization-defined time period*].

Supplemental Guidance: Resolution of input validation errors includes, for example, correcting systemic causes of errors and resubmitting transactions with corrected input.

(3) INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR

The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.

Supplemental Guidance: A common vulnerability in organizational information systems is unpredictable behavior when invalid inputs are received. This control enhancement ensures that there is predictable behavior in the face of invalid inputs by specifying information system responses that facilitate transitioning the system to known states without adverse, unintended side effects.

(4) INFORMATION INPUT VALIDATION | REVIEW / TIMING INTERACTIONS

The organization accounts for timing interactions among information system components in determining appropriate responses for invalid inputs.

Supplemental Guidance: In addressing invalid information system inputs received across protocol interfaces, timing interfaces become relevant, where one protocol needs to consider the impact of the error response on other protocols within the protocol stack. For example, 802.11 standard wireless network protocols do not interact well with Transmission Control Protocols (TCP) when packets are dropped (which could be due to invalid packet input). TCP assumes packet losses are due to congestion, while packets lost over 802.11 links are typically dropped due to collisions or noise on the link. If TCP makes a congestion response, it takes precisely the wrong action in response to a collision event. Adversaries may be able to use apparently acceptable individual behaviors of the protocols in concert to achieve adverse effects through suitable construction of invalid input.

(5) INFORMATION INPUT VALIDATION | RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS

The organization restricts the use of information inputs to [*Assignment: organization-defined trusted sources*] and/or [*Assignment: organization-defined formats*].

Supplemental Guidance: This control enhancement applies the concept of whitelisting to information inputs. Specifying known trusted sources for information inputs and acceptable formats for such inputs can reduce the probability of malicious activity.

References: None.

SI-11 ERROR HANDLING

Control: The information system:

a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and

b. Reveals error messages only to [*Assignment: organization-defined personnel or roles*].

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.

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.

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.

In the absence of AO specific guidance, National Archives and Records Administration (NARA) provide guidance on records retention.

Control Enhancements: None.

References: None.

SI-13 PREDICTABLE FAILURE PREVENTION

Control: The organization:

a. Determines mean time to failure (MTTF) for [*Assignment: organization-defined information system components*] in specific environments of operation; and

b. Provides substitute information system components and a means to exchange active and standby components at [*Assignment: organization-defined MTTF substitution criteria*].

Supplemental Guidance: While MTTF is primarily a reliability issue, this control addresses potential failures of specific information system components that provide security capability. Failure rates reflect installation-specific consideration, not industry-average. Organizations define criteria for substitution of information system components based on MTTF value with consideration for resulting potential harm from component failures. Transfer of responsibilities between active and standby components does not compromise safety, operational readiness, or security capability (e.g., preservation of state variables). Standby components remain available at all times except for maintenance issues or recovery failures in progress. Related controls: CP-2, CP-10, MA-6.

The standby component shall mirror the primary system. The organization develops this list of system components in support of availability requirements that have been identified from the Business Impact Analysis or local policy.

Control Enhancements:

(1) PREDICTABLE FAILURE PREVENTION | TRANSFERRING COMPONENT RESPONSIBILITIES

The organization takes information system components out of service by transferring component responsibilities to substitute components no later than [*Assignment: organization-defined fraction or percentage*] of mean time to failure.

(2) PREDICTABLE FAILURE PREVENTION | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION

[Withdrawn: Incorporated into SI-7 (16)].

(3) PREDICTABLE FAILURE PREVENTION | MANUAL TRANSFER BETWEEN COMPONENTS

The organization manually initiates transfers between active and standby information system components [*Assignment: organization-defined frequency*] if the mean time to failure exceeds [*Assignment: organization-defined time period*].

(4) PREDICTABLE FAILURE PREVENTION | STANDBY COMPONENT INSTALLATION / NOTIFICATION

The organization, if information system component failures are detected:

(a) Ensures that the standby components are successfully and transparently installed within [*Assignment: organization-defined time period*]; and

(b) [*Selection (one or more): activates* [*Assignment: organization-defined alarm*]; *automatically shuts down the information system*].

Supplemental Guidance: Automatic or manual transfer of components from standby to active mode can occur, for example, upon detection of component failures.

(5) PREDICTABLE FAILURE PREVENTION | FAILOVER CAPABILITY

The organization provides [*Selection: real-time; near real-time*] [*Assignment: organization-defined failover capability*] for the information system.

Supplemental Guidance: Failover refers to the automatic switchover to an alternate information system upon the failure of the primary information system. Failover capability includes, for example, incorporating mirrored information system operations at alternate processing sites or periodic data mirroring at regular intervals defined by recovery time periods of organizations.

References: None.

SI-14 NON-PERSISTENCE

Control: The organization implements non-persistent [*Assignment: organization-defined information system components and services*] that are initiated in a known state and terminated [*Selection (one or more): upon end of session of use; periodically at [Assignment: organization-defined frequency*]].

Supplemental Guidance: This control mitigates risk from advanced persistent threats (APTs) by significantly reducing the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber attacks. By implementing the concept of non-persistence for selected information system components, organizations can provide a known state computing resource for a specific period of time that does not give adversaries sufficient time on target to exploit vulnerabilities in organizational information systems and the environments in which those systems operate. Since the advanced persistent threat is a high-end threat with regard to capability, intent, and targeting, organizations assume that over an extended period of time, a percentage of cyber attacks will be successful. Non-persistent information system components and services are activated as required using protected information and terminated periodically or upon the end of sessions. Non-persistence increases the work factor of adversaries in attempting to compromise or breach organizational information systems.

Non-persistent system components can be implemented, for example, by periodically re-imaging components or by using a variety of common virtualization techniques. Non-persistent services can be implemented using virtualization techniques as part of virtual machines or as new instances of processes on physical machines (either persistent or non-persistent).The benefit of periodic refreshes of information system components/services is that it does not require organizations to first determine whether compromises of components or services have occurred (something that may often be difficult for organizations to determine). The refresh of selected information system components and services occurs with sufficient frequency to prevent the spread or intended impact of attacks, but not with such frequency that it makes the information system unstable. In some instances, refreshes of critical components and services may be done periodically in order to hinder the ability of adversaries to exploit optimum windows of vulnerabilities. Related controls: SC-30, SC-34.

Control Enhancements:

(1) NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES

The organization ensures that software and data employed during information system component and service refreshes are obtained from [*Assignment: organization-defined trusted sources*].

Supplemental Guidance: Trusted sources include, for example, software/data from write-once, read-only media or from selected off-line secure storage facilities.

References: None.

SI-15 INFORMATION OUTPUT FILTERING

Control: The information system validates information output from [*Assignment: organization-defined software programs and/or applications*] to ensure that the information is consistent with the expected content.

Supplemental Guidance: Certain types of cyber attacks (e.g., SQL injections) produce output results that are unexpected or inconsistent with the output results that would normally be expected from software programs or applications. This control enhancement focuses on detecting extraneous content, preventing such extraneous content from being displayed, and alerting monitoring tools that anomalous behavior has been discovered. Related controls: SI-3, SI-4.

Control Enhancements: None.

References: None.

SI-16 MEMORY PROTECTION

Control: The information system implements [*Assignment: organization-defined security safeguards*] to protect its memory from unauthorized code execution.

Supplemental Guidance: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism. Related controls: AC-25, SC-3.

Control Enhancements: None.

References: None.

SI-17 FAIL-SAFE PROCEDURES

Control: The information system implements [*Assignment: organization-defined fail-safe procedures*] when [*Assignment: organization-defined failure conditions occur*].

Supplemental Guidance: Failure conditions include, for example, loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include, for example, alerting operator personnel and providing specific instructions on subsequent steps to take (e.g., do nothing, reestablish system settings, shut down processes, restart the system, or contact designated organizational personnel). Related controls: CP-12, CP-13, SC-24, SI-13.

Control Enhancements: None.

References: None.

FAMILY: PROGRAM MANAGEMENT

PM-1 INFORMATION SECURITY PROGRAM PLAN

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.

> DoD SAP-specific 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. Reference the *Defense Acquisition Guidebook* for 'program security considerations' and DoDM 5205.07, *DoD SAP Security Manual* for additional guidance.

Control Enhancements: None.

References: None.

PM-2 SENIOR INFORMATION SECURITY OFFICER

Control: The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Supplemental Guidance: The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.

> The Senior Information Security Officer (SISO), also referred to as the Chief Information Security Officer (CISO), is appointed as indicated in Chapter 1 of this document, "with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program."

Control Enhancements: None.

References: None.

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.

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 OMB FISMA reporting requirements.

b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

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 findings 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.

PM-5 INFORMATION SYSTEM INVENTORY

Control: The organization develops and maintains an inventory of its information systems.

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 SAP information systems is maintained within SAP channels.

Control Enhancements: None.

References: Web: http://www.omb.gov.

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

Control: The organization develops, monitors, and reports on the results of information security measures of performance.

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.

<table><tr><td>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.:
• Percent of employees who received annual security awareness training.
• Percent of employees who received annual information assurance awareness training.
• 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.</td></tr></table>

Control Enhancements: None.

References: NIST Special Publication 800-55.

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.

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, an integral *information security architecture* consistent with organizational risk management and information security strategies. For PM-7, the information security architecture is developed at a system-of-systems level (organization-wide), representing all of the organizational information systems. For PL-8, the information security architecture is developed at a level representing an individual information system but at the same time, is consistent with the information security architecture defined for the organization. Security requirements and security control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures. 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.

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.

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, to address organizational changes.

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.

PM-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; and

c. Fully integrates the security authorization processes into an organization-wide risk management program.

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.

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.

PM-12 INSIDER THREAT PROGRAM

Control: The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

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-4(6) IR-4(7) IR-10 MP-2 MP-7 PE-3 PS-3 PS-4 SI-4 SC-28.

Control Enhancements: None.

References: Executive Order 13587.

PM-13 INFORMATION SECURITY WORKFORCE

Control: The organization establishes an information security workforce development and improvement program.

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:
>
> Privileged users have a working knowledge of system functions, security policies, technical security safeguards, and operational security measures. DoD has implemented its Workforce Improvement Program through DoD 8570.01-M and its follow-on DoDD 8140.01.
>
> 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.

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.

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.

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.

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:
>
> - System Administration, Networking, and Security (SANS) Institute.
> - Conferences such as the DoD IA Conference.
> - Contractor SAP Security Working Group (CSSWG).
>
> IA and Computer Network Defense (CND) personnel and Service CISOs 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.

PM-16 THREAT AWARENESS PROGRAM

Control: The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

Supplemental Guidance: Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared. Related controls: PM-12, PM-16.

Control Enhancements: None.

References: None.

Privacy Families

AP	Authority and Purpose
AR	Accountability, Audit, and Risk Management
DI	Data Quality and Integrity
DM	Data Minimization and Retention
IP	Individual Participation and Redress
SE	Security
TR	Transparency
UL	Use Limitation

Table 3-5: Privacy Control Families and Identifiers

FAMILY: AUTHORITY AND PURPOSE

> This family ensures that organizations: (i) identify the legal bases that authorize a particular personally identifiable information (PII) collection or activity that impacts privacy; and (ii) specify in their notices the purpose(s) for which PII is collected.

AP-1 AUTHORITY TO COLLECT

Control: The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.

Supplemental Guidance: Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements. Related controls: AR-2, DM-1, TR-1, TR-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Circular A-130, Appendix I.

AP-2 PURPOSE SPECIFICATION

Control: The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

Supplemental Guidance: Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII). Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice. 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 of 2002 (P.L. 107-347).

FAMILY: ACCOUNTABILITY, AUDIT AND RISK MANAGEMENT

This family enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk.

AR-1 GOVERNANCE AND PRIVACY PROGRAM

Control: The organization:

a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems;

b. Monitors federal privacy laws and policy for changes that affect the privacy program;

c. Allocates [*Assignment: organization-defined allocation of budget and staffing*] sufficient resources to implement and operate the organization-wide privacy program;

d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;

e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and

f. Updates privacy plan, policies, and procedures **at least biennially**.

Sufficient resources to meet AR-1.c are generally downward directed by service/agency or corporate entities.

Supplemental Guidance: The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of an SAOP/CPO with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SAOP/CPO, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development, implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls.

To further accountability, the SAOP/CPO develops privacy plans to document the privacy requirements of organizations and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of organizational privacy operations and supports resource requests by the SAOP/CPO. A single plan or multiple plans may be necessary depending upon the organizational structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as Privacy Impact Assessments (PIA) and System of Records Notices (SORN). A comprehensive plan may include a baseline of privacy controls selected from this appendix and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls. Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 03-22, 05-08, 07-16; OMB Circular A-130; Federal Enterprise Architecture Security and Privacy Profile.

AR-2 PRIVACY IMPACT AND RISK ASSESSMENT

Control: The organization:

a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and

b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Supplemental Guidance: Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. They include, but are not limited to, the conduct of PIAs. The PIA is both a process and the document that is the outcome of that process. OMB Memorandum 03-22 provides guidance to organizations for implementing the privacy provisions of the E-Government Act of 2002, including guidance on when PIAs are required for information systems. Some organizations may be required by law or policy to extend the PIA requirement to other activities involving PII or otherwise impacting privacy (e.g., programs, projects, or regulations). PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information systems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public of privacy practices. PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.

Section 208 of the E-Government Act of 2002 and Section 522 of the Consolidated Appropriations Act of 2005 require protection of PII. PII is defined [in CNSSI 4009] as information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. When developing or procuring information systems that collect, use, store, and/or disclose PII, potential privacy risks must be identified and appropriate privacy controls implemented.

The SSP for the information system shall indicate whether the system "does" or "does not" contain privacy information. If the information system contains privacy information, the ISO must contact a DoD SAP cleared PII POC to determine PIA requirements in accordance with OMB policy.

Control Enhancements: None.

References: Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 03-22, 05-08, 10-23.

AR-3 PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS

Control: The organization:

a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and

b. Includes privacy requirements in contracts and other acquisition-related documents.

Supplemental Guidance: Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control. Related control: AR-1, AR-5, SA-4.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a(m); Federal Acquisition Regulation, 48 C.F.R. Part 24; OMB Circular A-130.

AR-4 PRIVACY MONITORING AND AUDITING

Control: The organization monitors and audits privacy controls and internal privacy policy **continuously** to ensure effective implementation.

Supplemental Guidance: To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems. In addition to auditing for effective implementation of all privacy controls identified in this appendix, organizations assess whether they: (i) implement a process to embed privacy considerations into the life cycle of personally identifiable information (PII), programs, information systems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations, and policies; (iii) track programs, information systems, and applications that collect and maintain PII to ensure compliance; (iv) ensure that access to PII is only on a *need-to-know* basis; and (v) ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s).

Organizations also: (i) implement technology to audit for the security, appropriate use, and loss of PII; (ii) perform reviews to ensure physical security of documents containing PII; (iii) assess contractor compliance with privacy requirements; and (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials. Related controls: AR-6, AR-7, AU-1, AU-2, AU-3, AU-6, AU-12, CA-7, TR-1, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 05-08, 06-16, 07-16; OMB Circular A-130.

AR-5 PRIVACY AWARENESS AND TRAINING

Control: The organization:

a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;

b. Administers basic privacy training **at least annually** and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII **at least annually**; and

c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements **at least annually**.

Supplemental Guidance: Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act of 2002 and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use requirements identified in public notices, such as Privacy Impact Assessments (PIAs) or System of Records Notices (SORNs) for a program or information system. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program websites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors. Organizations update training based on changing statutory, regulatory, mission, program, business process, and information system requirements, or on the results of compliance monitoring and auditing. Where appropriate, organizations may provide privacy training as part of existing information security training. Related controls: AR-3, AT-2, AT-3, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a(e); Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16.

AR-6 PRIVACY REPORTING

Control: The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Supplemental Guidance: Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Types of privacy reports include: (i) annual Senior Agency Official for Privacy (SAOP) reports to OMB; (ii) reports to Congress required by the *Implementing Regulations of the 9/11 Commission Act*; and (iii) other public reports required by specific statutory mandates or internal policies of organizations. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 803, 9/11 Commission Act, 42 U.S.C. § 2000ee-1; Section 804, 9/11 Commission Act, 42 U.S.C. § 2000ee-3; Section 522, Consolidated Appropriations Act of 2005 (P.L. 108-447); OMB Memoranda 03-22; OMB Circular A-130.

AR-7 PRIVACY-ENHANCED SYSTEM DESIGN AND DEVELOPMENT

Control: The organization designs information systems to support privacy by automating privacy controls.

Supplemental Guidance: To the extent feasible, when designing organizational information systems, organizations employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, organizations mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents. Organizations also conduct periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act and the organization’s privacy policy. Regardless of whether automated privacy controls are employed, organizations regularly monitor information system use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notice of organizations, or in a manner compatible with those purposes. Related controls: AC-6, AR-4, AR-5, DM-2, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a(e)(10); Sections 208(b) and(c), E-Government Act of 2002 (P.L. 107-347); OMB Memorandum 03-22.

AR-8 ACCOUNTING OF DISCLOSURES

Control: The organization:

a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:

   (1) Date, nature, and purpose of each disclosure of a record; and

   (2) Name and address of the person or agency to which the disclosure was made;

b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and

c. Makes the accounting of disclosures available to the person named in the record upon request.

Supplemental Guidance: The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) periodically consults with managers of organization systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.S.C. § 552a(c)(3). Heads of agencies can promulgate rules to exempt certain systems of records from the requirement to provide the accounting of disclosures to individuals. Related control: IP-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (c)(1), (c)(3), (j), (k).

FAMILY: DATA QUALITY AND INTEGRITY

> This family enhances public confidence that any personally identifiable information (PII) collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.

DI-1 DATA QUALITY

Control: The organization:

a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;

b. Collects PII directly from the individual to the greatest extent practicable;

c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems **at least every 180 days**; and

d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Supplemental Guidance: Organizations take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.

When PII is of a sufficiently sensitive nature (e.g., when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit), organizations incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated. Related controls: AP-2, DI-2, DM-1, IP-3, SI-10.

Control Enhancements:

(1) *DATA QUALITY | VALIDATE PII*

The organization requests that the individual or individual's authorized representative validate PII during the collection process.

(2) *DATA QUALITY | RE-VALIDATE PII*

The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate [*Assignment: organization-defined frequency*].

References: The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB Memorandum 07-16**.**

DI-2 DATA INTEGRITY AND DATA INTEGRITY BOARD

Control: The organization:

a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and

b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements[123] and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

Supplemental Guidance: Organizations conducting or participating in Computer Matching Agreements with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. In many organizations, the Data Integrity Board is led by the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO). The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under Computer Matching Agreements. Related controls: AC-1, AC-3, AC-4, AC-6, AC-17, AC-22, AU-2, AU-3, AU-6, AU-10, AU-11, DI-1, SC-8, SC-28, UL-2.

Control Enhancements:

(1) *DATA INTEGRITY AND DATA INTEGRITY BOARD* | *PUBLISH AGREEMENTS ON WEBSITE*

The organization publishes Computer Matching Agreements on its public website.

References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (a)(8)(A), (o), (p), (u); OMB Circular A-130, Appendix I.

123 Organizations enter into Computer Matching Agreements in connection with computer matching programs to which they are a party. With certain exceptions, a computer matching program is any computerized comparison of two or more automated systems of records or a system of records with nonfederal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance or payments under federal benefit programs or computerized comparisons of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with nonfederal records. See Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a (a)(8)(A).

FAMILY: DATA MINIMIZATION AND RETENTION

This family helps organizations implement the data minimization and retention requirements to collect, use, and retain only personally identifiable information (PII) that is relevant and necessary for the purpose for which it was originally collected. Organizations retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

DM-1 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION

Control: The organization:

a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and

c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings **at least annually** to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Supplemental Guidance: Organizations take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose.

Organizations can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. OMB Memorandum 07-16 requires organizations to conduct both an initial review and subsequent reviews of their holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Organizations are also directed by OMB to reduce their holdings to the minimum necessary for the proper performance of a documented organizational business purpose. OMB Memorandum 07-16 requires organizations to develop and publicize, either through a notice in the Federal Register or on their websites, a schedule for periodic reviews of their holdings to supplement the initial review. Organizations coordinate with their federal records officers to ensure that reductions in organizational holdings of PII are consistent with NARA retention schedules.

By performing periodic evaluations, organizations reduce risk, ensure that they are collecting only the data specified in the notice, and ensure that the data collected is still relevant and necessary for the purpose(s) specified in the notice. Related controls: AP-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1.

Control Enhancements:

(1) *MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION | LOCATE / REMOVE / REDACT / ANONYMIZE PII*

The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

Supplemental Guidance: NIST Special Publication 800-122 provides guidance on anonymization.

References: The Privacy Act of 1974, 5 U.S.C. §552a (e); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16.

DM-2 DATA RETENTION AND DISPOSAL

Control: The organization:

a. Retains each collection of personally identifiable information (PII) for **in accordance with National Archives and Records Administration (NARA)** to fulfill the purpose(s) identified in the notice or as required by law;

b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

c. Uses [*Assignment: organization-defined techniques or methods*] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Supplemental Guidance: NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper.

Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII.

Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may not permit the removal of individual records without the destruction of the entire database contained on such media. Related controls: AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1.

In reference to DM-2.c, unless otherwise directed destruction methods used for classified data meet or exceed destruction of PII data.

Control Enhancements:

(1) *DATA RETENTION AND DISPOSAL* | *SYSTEM CONFIGURATION*

The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(1), (c)(2); Section 208 (e), E-Government Act of 2002 (P.L. 107-347); 44 U.S.C. Chapters 29, 31, 33; OMB Memorandum 07-16; OMB Circular A-130; NIST Special Publication 800-88.

DM-3 MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH

Control: The organization:

a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and

b. Implements controls to protect PII used for testing, training, and research.

Supplemental Guidance: Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. Organizations consult with the SAOP/CPO and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected.

Control Enhancements:

(1) *MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH | RISK MINIMIZATION TECHNIQUES*

The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

Supplemental Guidance: Organizations can minimize risk to privacy of PII by using techniques such as de-identification.

References: NIST Special Publication 800-122.

FAMILY: INDIVIDUAL PARTICIPATION AND REDRESS

> This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their personally identifiable information (PII). By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII.

IP-1 CONSENT

Control: The organization:

a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;

b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;

c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and

d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Supplemental Guidance: Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices.

Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to *allow* organizations to collect or use PII. For example, opt-in consent may require an individual to click a radio button on a website, or sign a document providing consent. In contrast, opt-out requires individuals to take action to *prevent* the new or continued collection or use of such PII. For example, the Federal Trade Commission's Do-Not-Call Registry allows individuals to opt-out of receiving unsolicited telemarketing calls by requesting to be added to a list. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. Organizational consent mechanisms include a discussion of the consequences to individuals of failure to provide PII. Consequences can vary from organization to organization. Related controls: AC-2, AP-1, TR-1, TR-2.

Control Enhancements:

(1) *CONSENT | MECHANISMS SUPPORTING ITEMIZED OR TIERED CONSENT*

The organization implements mechanisms to support itemized or tiered consent for specific uses of data.

Supplemental Guidance: Organizations can provide, for example, individuals' itemized choices as to whether they wish to be contacted for any of a variety of purposes. In this situation, organizations construct consent mechanisms to ensure that organizational operations comply with individual choices.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 10-22.

IP-2 INDIVIDUAL ACCESS

Control: The organization:

a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;

b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;

c. Publishes access procedures in System of Records Notices (SORNs); and

d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Supplemental Guidance: Access affords individuals the ability to review PII about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Access to certain types of records may not be appropriate, however, and heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act. In addition, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding. Related controls: AR-8, IP-3, TR-1, TR-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4); (j), (k), (t); OMB Circular A-130.

IP-3 REDRESS

Control: The organization:

a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and

b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

Supplemental Guidance: Redress supports the ability of individuals to ensure the accuracy of PII held by organizations. Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate.

To provide effective redress, organizations: (i) provide effective notice of the existence of a PII collection; (ii) provide plain language explanations of the processes and mechanisms for requesting access to records; (iii) establish criteria for submitting requests for correction or amendment; (iv) implement resources to analyze and adjudicate requests; (v) implement means of correcting or amending data collections; and (vi) review any decisions that may have been the result of inaccurate information.

Organizational redress processes provide responses to individuals of decisions to deny requests for correction or amendment, including the reasons for those decisions, a means to record individual objections to the organizational decisions, and a means of requesting organizational reviews of the initial determinations. Where PII is corrected or amended, organizations take steps to ensure that all authorized recipients of that PII are informed of the corrected or amended information. In instances where redress involves information obtained from other organizations, redress processes include coordination with organizations that originally collected the information. Related controls: IP-2, TR-1, TR-2, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (d), (c)(4); OMB Circular A-130.

IP-4 COMPLAINT MANAGEMENT

Control: The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Supplemental Guidance: Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards. Organizations provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) or other official designated to receive complaints), and are easy to use. Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner. Related controls: AR-6, IP-3.

Control Enhancements:

(1) *COMPLAINT MANAGEMENT | RESPONSE TIMES*

The organization responds to complaints, concerns, or questions from individuals within **two (2) business days.**

References: OMB Circular A-130; OMB Memoranda 07-16, 08-09.

FAMILY: SECURITY

> This family supplements the security controls in Appendix F to ensure that technical, physical, and administrative safeguards are in place to protect personally identifiable information (PII) collected or maintained by organizations against loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework.

SE-1 INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

Control: The organization:

a. Establishes, maintains, and updates **at least annually** an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and

b. Provides each update of the PII inventory to the CIO or information security official **at least annually** to support the establishment of information security requirements for all new or modified information systems containing PII.

Supplemental Guidance: The PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII consistent with Appendix F, and to mitigate risks of PII exposure. As one method of gathering information for their PII inventories, organizations may extract the following information elements from Privacy Impact Assessments (PIA) for information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Organizations take due care in updating the inventories by identifying linkable data that could create PII. Related controls: AR-1, AR-4, AR-5, AT-1, DM-1, PM-5.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e) (10); Section 208(b)(2), E-Government Act of 2002 (P.L. 107-347); OMB Memorandum 03-22; OMB Circular A-130, Appendix I; FIPS Publication 199; NIST Special Publications 800-37, 800-122.

SE-2 PRIVACY INCIDENT RESPONSE

Control: The organization:

a. Develops and implements a Privacy Incident Response Plan; and

b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

Supplemental Guidance: In contrast to the Incident Response (IR) family in Appendix F, which concerns a broader range of incidents affecting information security, this control uses the term Privacy Incident to describe only those incidents that relate to personally identifiable information (PII). The organization Privacy Incident Response Plan is developed under the leadership of the SAOP/CPO. The plan includes: (i) the establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan; (ii) a process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly; (iii) a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; (iv) internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), consistent with organizational incident management structures; and (v) internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials. Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a breach. Organizations may also choose to integrate Privacy Incident Response Plans with Security Incident Response Plans, or keep the plans separate. Related controls: AR-1, AR-4, AR-5, AR-6, AU-1 through 14, IR-1 through IR-8, RA-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e), (i)(1), and (m); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 06-19, 07-16; NIST Special Publication 800-37.

FAMILY: TRANSPARENCY

> This family ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities.

TR-1 PRIVACY NOTICE

Control: The organization:

a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;

b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and

c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Supplemental Guidance: Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices. The organization may provide general public notice through a variety of means, as required by law or policy, including System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), or in a website privacy policy. As required by the Privacy Act, the organization also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.

The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of the organization's public notices, in consultation with legal counsel and relevant program managers. The public notice requirement in this control is satisfied by an organization's compliance with the public notice provisions of the Privacy Act, the E-Government Act's PIA requirement, with OMB guidance related to federal agency privacy notices, and, where applicable, with policy pertaining to participation in the Information Sharing Environment (ISE).[124] Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SAOP/CPO and counsel. Related controls: AP-1, AP-2, AR-1, AR-2, IP-1, IP-2, IP-3, UL-1, UL-2.

124 The Information Sharing Environment is an approach that facilitates the sharing of terrorism and homeland security information. The ISE was established by the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, 118 Stat. 3638. See the ISE website at: http://www.ise.gov.

Control Enhancements:

(1) *PRIVACY NOTICE* | *REAL-TIME OR LAYERED NOTICE*

The organization provides real-time and/or layered notice when it collects PII.

Supplemental Guidance: Real-time notice is defined as notice at the point of collection. A layered notice approach involves providing individuals with a summary of key points in the organization's privacy policy. A second notice provides more detailed/specific information.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16, 10-22, 10-23; ISE Privacy Guidelines.

TR-2 SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS

Control: The organization:

a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);

b. Keeps SORNs current; and

c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

Supplemental Guidance: Organizations issue SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as "a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier." SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. Privacy Act Statements provide notice of: (i) the authority of organizations to collect PII; (ii) whether providing PII is mandatory or optional; (iii) the principal purpose(s) for which the PII is to be used; (iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information requested. When information is collected verbally, organizations read a Privacy Act Statement prior to initiating the collection of PII (for example, when conducting telephone interviews or surveys). Related control: DI-2.

Control Enhancements:

(1) *SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS* | *PUBLIC WEBSITE PUBLICATION*

The organization publishes SORNs on its public website.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3); OMB Circular A-130.

TR-3 DISSEMINATION OF PRIVACY PROGRAM INFORMATION

Control: The organization:

a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and

b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Supplemental Guidance: Organizations employ different mechanisms for informing the public about their privacy practices including, but not limited to, Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). Organizations also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices. Related control: AR-6.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 10-23.

FAMILY: USE LIMITATION

> This family ensures that organizations only use personally identifiable information (PII) either as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly.

UL-1 INTERNAL USE

Control: The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Supplemental Guidance: Organizations take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII. With guidance from the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and where appropriate, legal counsel, organizations document processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new use(s) of PII. Related controls: AP-2, AR-2, AR-3, AR-4, AR-5, IP-1, TR-1, TR-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (b)(1).

UL-2 INFORMATION SHARING WITH THIRD PARTIES

Control: The organization:

a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;

b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;

c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and

d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Supplemental Guidance: The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act and/or specified in a notice, organizations evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, organizations review, update, and republish their Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared. Related controls: AR-3, AR-4, AR-5, AR-8, AP-2, DI-1, DI-2, IP-1, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines.

APPENDIX A: References

Federal Publications

http://www.whitehouse.gov/omb/memoranda_default/
http://www.archives.gov/records-mgmt/grs/

- Presidential Memo, *National Insider Threat Policy and Minimum Standards for Insider Threat Programs,* November 21, 2012.
- *Consolidated Appropriations Act of 2005,* Section 522.
- *E-Government Act of 2002,* Section 208.
- *Federal Information Security Management Act of 2002*, December 17, 2002, which is Title III of *E-Government Act of 2002*.
- OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 30, 2003.
- OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007.
- NARA, *General Records Schedules*, *Electronic Records*, Transmittal No. 22, April 2010.

Chairman of the Joint Chiefs of Staff (CJCS) Publications

http://www.dtic.mil/cjcs_directives/

- CJCSM 6510.01B, *Cyber Incident Handling Program*, July 10, 2012, current as of December 18, 2014.

Office of the Director of National Intelligence (ODNI) Publications

http://www.dni.gov/index.php/intelligence-community/ic-policies-reports

- ICD 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*, September 15, 2008.

Committee on National Security Systems (CNSS) Publications

http://www.cnss.gov

- CNSSP 15, *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems*, October 1, 2012.
- CNSSP 26, *National Policy on Reducing the Risk of Removable Media for National Security Systems*, July 25, 2013 (FOUO).
- CNSSP 300, *National Policy on Control of Compromising Emanations*, January 11, 2006 (FOUO).
- CNSSD 505, *Supply Chain Risk Management*, March 7, 2012 (FOUO).
- CNSSI 1253, *Security Categorization and Control Selection for National Security Systems*, March 27, 2014.
- CNSSI 4009, *Committee on National Security Systems Glossary*, April 6, 2015.
- CNSSI 7000, *TEMPEST Countermeasures for Facilities*, C//Rel, May 2004.
- NSTISSI 7001, *NONSTOP Countermeasures*, S//NOFORN, June 15, 1994.

- CNSSI 7003, *Protective Distribution Systems (PDS)*, September 30, 2015.
- CNSSAM TEMPEST/1-13, *Red/Black Installation Guidelines*, U//FOUO, January 17, 2014.

Department of Defense (DoD) Publications (numeric order)
http://www.dtic.mil/whs/directives/index.html

- DoDD 5000.01, *The Defense Acquisition Systems*, May 12, 2003, certified current as of November 20, 2007.
- DoDM 5200.01 Volume 3, *DoD Information Security Program: Protection of Classified Information*, February 24, 2012.
- DoDI 5000.02, *Operation of the Defense Acquisition System*, January 7, 2008.
- DoDI 5200.39, *Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)*, May 28, 2015.
- DoDD 5205.07, *Special Access Program (SAP) Policy*, July 1, 2010.
- DoDM 5205.07 Volume 1, *DoD Special Access Program (SAP) Security Manual: General Procedures*, June 18, 2015.
- DoDM 5205.07 Volume 2, *DoD Special Access Program (SAP) Security Manual: Personnel Security*, November 24, 2015.
- DoDM 5205.07 Volume 3, *DoD Special Access Program (SAP) Security Manual: Physical Security*, April 23, 2015.
- DoDM 5205.07 Volume 4, *DoD Special Access Program (SAP) Security Manual: Marking*, October 10, 2013.
- DoDI 5205.11, *Management, Administration, and Oversight of DoD Special Access Programs (SAPs)*, February 6, 2013.
- DoDD 5205.16, *The DoD Insider Threat Program*, September 30, 2014.
- DoDD 8140.01, *Cybersecurity Workforce Management*, August 11, 2015.
- DoDI 8500.01, *Cybersecurity*, March 14, 2014.
- DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, March 12, 2014.
- DoDD 8523.01, *Communications Security (COMSEC)*, April 22, 2008.
- DoDI 8551.1, *Ports, Protocols, and Services Management (PPSM)*, May 28, 2014.
- DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, December 19, 2005; Change 3, January 24, 2012. (This document will be superseded by direction of DoDD 8140.01.)
- *Defense Acquisition Guidebook*, updated continuously at https://dag.dau.mil.
- DISA, *Voice and Video Over IP (VVoIP) STIG*, Version 3, Release 6, July 24, 2015.
- DISA IASE, http://iase.disa.mil/Pages/index.aspx

- JSIG Templates located on JAFAN Community Website.
    - o https://intelshare.intelink.gov/sites/jafan (Access restricted to users supporting DoD SAP Community, requires DoD CAC or Remote Access credentials, Intelink-U account (https://www.intelink.gov), and approved access.)
- OSD Memo for SAP Senior Working Group Members, *Transition to the Risk Management Framework*, December 18, 2013.
- OSD Memo: Approval for use of DoD SAPFs and SAPCAs as SAPWAs for all DoD SAPs, December 10, 2015.
- OSD Memo for SAP Senior Working Group, *Reciprocity of DoD SAPF Accreditations*, January 7, 2016.

NSA Publications

http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/

- NSA/CSS Policy Manual 9-12, *Storage Device Declassification Manual (SDDM),* December 14, 2014.
- NSA/CSS *Degausser Evaluated Products List*, August 24, 2015.
- NSA/CSS *Evaluated Products List for Optical Media Destruction Devices*, May 15, 2015.

NIST Publications

http://csrc.nist.gov/publications/PubsSPs.html

http://csrc.nist.gov/publications/PubsFIPS.html

* Joint Task Force (JTF) Document

- FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001; Change notice December 3, 2002.
- NIST SP 800-30*, Revision 1, *Guide for Conducting Risk Assessments*, September 2012.
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010 (Updates November 11, 2010).
- NIST SP 800-37*, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010 (Updates June 5, 2014).
- NIST SP 800-39* *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.
- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.
- NIST SP 800-48, Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, July 2008.
- NIST SP 800-53*, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (Updates as of January 22, 2015).
- NIST SP 800-53A*, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, December 2014.

- NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security*, July 2008.
- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
- NIST SP 800-60, Revision 1, Volume 1, *Guide for Mapping Types of Information and Information Systems to Security Categories,* Volume 2: *Appendices*, Aug 2008.
- NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, August 2012.
- NIST SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008.
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems,* August 2011.
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations,* September 2011.
- NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015.
- NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, April 2015.

APPENDIX B: Acronyms

AC	Access Control (Security Control Family)
ACERT-CNO	Army Computer Emergency Response Team - Computer Network Operations
AFNOSC NSD	Air Force Network Operations and Security Center Network Security Division
AFT	Assured File Transfer
AO	Authorizing Official
AP	Authority and Purpose (Privacy Family)
AR	Accountability, Audit, and Risk Management (Privacy Family)
AT	Awareness and Training (Security Control Family)
ATC	Authorization to Connect
ATO	Authorization to Operate
AU	Audit and Accountability (Security Control Family)
BCP	Business Continuity Plan
BIA	Business Impact Analysis
C&A	Certification and Accreditation
CA	Cognizant Authority
CA	Security Assessment and Authorization (Security Control Family)
CAC	Common Access Card
CCB	Configuration Control Board
CCP	Common Control Provider
CD	Compact Disc
CDR	Critical Design Review
CDS	Cross Domain Solution
CDSE	Center for Development of Security Excellence
CDSE	Cross Domain Support Element
CERT	Computer Emergency Response (or Readiness) Team
CI	Controlled Interface
CI	Counterintelligence (Notice and Consent Banner)
CIAO	Chief Information Assurance Officer (New term: CISO)

CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CM	Configuration Management (also a Security Control Family)
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COMSEC	Communications Security
ConMon	Continuous Monitoring
CONOPS	Concept of Operations
COOP	Continuity of Operations, Continuity of Operations Plan
COTS	Commercial-off-the-Shelf
CP	Contingency Planning (Security Control Family)
CPSO	Contractor Program Security Officer
CSA	Cognizant Security Authority
CSIRT	Computer Security Incident Response Team
CSS	Central Security Service
CSSWG	Contractor SAP Security Working Group
CT&E	Certification Test and Evaluation (New report: SAR)
CTO	Communications Tasking Order
CTTA	Certified TEMPEST Technical Authority
CUI	Controlled Unclassified Information
DAA	Designated Accrediting Authority (New term: AO)
DAA Rep	Designated Accrediting Authority Representative
DAC	Discretionary Access Control
DAO	Delegated Authorizing Official

DARPA	Defense Advanced Research Projects Agency
DATO	Denied Authorization to Operate
DFAR	Defense Federal Acquisition Regulation
DI	Data Quality and Integrity (Privacy Family)
DISA	Defense Information Systems Agency
DM	Data Minimization and Retention (Privacy Family)
DNI	Director of National Intelligence
DNS	Domain Name System
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual
DRP	Disaster Recovery Plan
DS	Delegation Signer
DSS	Defense Security Service
DTA	Data Transfer Agent
DVD	Digital Versatile Disk
EAL	Evaluation Assurance Level
EO	Executive Order
EPL	Evaluated Products List
EPROM	Erasable PROM
FAQ	Frequently Asked Questions
FAR	Federal Acquisition Regulation
FDO	Foreign Disclosure Office
FFC	Fixed Facility Checklist
FIPS or FIPS PUB	Federal Information Processing Standard Publication
FISMA	Federal Information Security Management Act
FOCI	Foreign Ownership, Control and Influence
FOUO	For Official Use Only
FPGA	Field Programmable Gate Array

FTP	File Transfer Protocol
FWAC	Fraud, Waste and Abuse Center
GOTS	Government off-the-shelf
GSSO	Government SAP Security Officer
HID	Human Interface Device
HSPD	Homeland Security Presidential Directive
HVSACO	Handle Via Special Access Channels Only
I/O	Input/Output (e.g., I/O Port)
IA	Identification and Authentication (Security Control Family)
IA	Information Assurance
IA SOP	Information Assurance Stand Operating Procedures
IAM	Information Assurance Manager (New term: ISSM)
IAO	Information Assurance Officer (New term: ISSO)
IASAE	Information Assurance Systems Architect and Engineer, see ISSE
IASE	Information Assurance Support Environment
IATT	Interim Authorization to Test
IAV	Information Assurance Vulnerability
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
IAVT	Information Assurance Vulnerability Technical Advisory
IC	Intelligence Community
IC-SCC	Intelligence Community Security Coordination Center
ICD	Intelligence Community Directive
ICVA	Intelligence Community Vulnerability Alerts
ICVM	Intelligence Community Vulnerability Management
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IG	Inspectors General
IP	Individual Participation and Redress (Privacy Family)

IP	Internet Protocol
IR	Incident Response (also a Security Control Family)
IR	Infrared
IS	Information System
ISA	Interconnection Security Agreement
ISC	Internet Storm Center
ISCM	Information Security Continuous Monitoring, see ConMon
ISCP	Information System Contingency Plan
ISO	Information System Owner
ISSE	Information System Security Engineer
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISSP	Information System Security Professional (New term: SCA)
IT	Information Technology
JAFAN	Joint Air Force – Army - Navy
JSCS WG	Joint SAP Cybersecurity Working Group
JSIG	Joint SAP Implementation Guide
JTF	Joint Task Force
JTF-GNO	Joint Task Force Global Network Operations
JWICS	Joint Worldwide Intelligence Communications System
KVM	Keyboard/Video/Mouse
LAN	Local Area Network
LE	Law Enforcement (Notice and Consent Banner)
LRU	Lowest Replaceable Unit
MA	Maintenance (Security Control Family)
MAC	Mandatory Access Control
MAC	Media Access Control
MBO	Mission/Business Owner
MCNOSC	Marine Corps Network Operations and Security Center
MDA	Missile Defense Agency

MOU	Memorandum of Understanding
MP	Media Protection (Security Control Family)
MSSP	Master System Security Plan (New term: IA SOP)
NAC	Network Access Control
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NCDOC	Navy Cyber Defense Operations Command
NIAP	National Information Assurance Program
NIPRNet	Non-secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NOFORN	Not releasable to foreign nationals
NSA	National Security Agency
NSPD	National Security Presidential Directive
NSS	National Security System
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OA	Oversight Authority
OCA	Original Classification Authority
ODNI	Office of the Director of National Intelligence
OEP	Occupant Emergency Plan
OMB	Office of Management and Budget
OPSEC	Operations Security
OS	Operating System
OSD	Office of the Secretary of Defense
OSS	Open Source Software
PDA	Personal Digital Assistant
PDR	Preliminary Design Review
PDS	Protected Distribution System
PE	Physical and Environmental Protection (Security Control Family)
PED	Portable Electronic Device
PIA	Privacy Impact Assessment

PII	Personally Identifiable Information
PIN	Personal Identification Number
PIT	Platform Information Technology
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	Planning (Security Control Family)
PL	Protection Level (New term: Impact Level)
PM	Personnel Misconduct (Notice and Consent Banner)
PM	Program Management (Security Control Family)
PM	Program Manager (aka ISO)
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPS	Ports, Protocols, and Services
PPSM	Ports, Protocols, and Services Management
PROM	Programmable Read-Only Memory
PS	Personnel Security (Security Control Family)
PSA	Principal Staff Assistant
PSO	Program Security Officer
R&D	Research and Development
RA	Risk Assessment (Security Control Family)
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RAR	Risk Assessment Report
RDT&E	Research Development Test and Evaluation
REF or REf	Risk Executive (function)
REL	Releasable
RF	Radio Frequency
RFID	Radio Frequency Identification
RMAT	Remote Maintenance and Testing
RMF	Risk Management Framework

ROM	Read Only Memory
S	Secret
S&T	Science and Technology
SA	System Administrator
SA	System and Services Acquisition (Security Control Family)
SAMI	Sources and Methods Intelligence
SANS	System Administration, Networking, and Security (Institute)
SAP	Special Access Program
SAPCA	Special Access Program Compartmented Area
SAPCO	Special Access Program Central Office
SAPF	Special Access Program Facility
SAPWA	Special Access Program Working Area
SAR	Security Assessment Report or Special Access Required
SBA	Site-Base Authorization
SC	System and Communication Protection (Security Control Family)
SCA	Security Control Assessor
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol (pronounced S-CAP)
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCO	Service Certifying Organization (New term: SCA)
SCTM	Security Controls Traceability Matrix
SDLC	System Development Life Cycle
SE	Security (Privacy Family)
SF	Standard Form
SI	System and Information Integrity (Security Control Family)
SIPRNet	Secure Internet Protocol Router Network
SISO	Senior Information Security Officer, see CISO
SME	Subject Matter Expert

SOP	Standard Operating Procedures
SOW	Statement of Work
SP	Special Publication
SRG	Security Requirements Guide
SRTM	Security Requirements Traceability Matrix (New term: SCTM)
SSAA	System Security Authorization Agreement (New term: SSP)
SSO	Special Security Office(r)
SSP	System Security Plan
ST&E	Security Test and Evaluation (New report: SAR)
STE	Secure Terminal Equipment
STIG	Security Technical Implementation Guide
TCP/IP	Transmission Control Protocol/Internet Protocol
TCR	TEMPEST Countermeasures Review
TEMPEST	(Not an acronym)
TLS	Transport Layer Security
TPM	Trusted Platform Module
TR	Transparency (Privacy Family)
TRQ	TEMPEST Requirements Questionnaire
TS	Top Secret
TSCA	Top Secret Control Account
TSCO	Top Secret Control Officer
U	Unclassified
UAC	User Account Control
UCDMO	Unified Cross Domain Management Office, see UCDSMO
UCDSMO	Unified Cross Domain Services Management Office, formerly UCDMO
UHF/VHF	Ultra High Frequency/Very High Frequency
UII	Unified Industries Incorporated
UL	Use Limitation (Privacy Family)
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus

USERID	User Identifier
USG	U.S. Government
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconference
VVoIP	Video and Voice Over Internet Protocol
WAN	Wide Area Network
WYSIWYG	What you see is what you get

APPENDIX C: SAP Security Control Baselines

The table that follows provides the security control selections for the DoD SAP Community and for all information systems under the purview of the CA SAPCO. This table is to be used in conjunction with information system security categorization to determine the baseline set of security controls applicable to an information system. See [RA-2] for detailed information pertaining to security categorization.

Security categorization results in the identification of the security impact level for each of the three information system security objectives: confidentiality, integrity and availability. Security impact levels are defined as low (L), moderate (M) or high (H) for each system security objective. The table indicates the security controls associated with each impact level for confidentiality, integrity and availability, shown as C, I, and A within the table heading. Security controls not selected as part of any baseline contain no entries within the C, I, and A columns and are included for reference and possible selection during the tailoring process. Security controls with an “S” in the C, I, or A columns apply specifically to SAP systems.

Security controls shall be documented in the Security Controls Traceability Matrix (SCTM), which can be created from the table below by deleting those columns associated with impact levels that do not apply to the information system. This provides the baseline set of security controls applicable to the information system which may require tailoring and/or supplementing based on other factors such as the information system usage, information owner requirements or the environment. This is especially true for tactical systems, standalone systems, embedded systems and others. If a security control identified in the baseline set of controls is tailored out, an explanation must be provided in the SCTM, describing the rationale as to why the control does not apply or how it is satisfied by other mitigating factors. Security controls may also be tailored in (i.e., added) as necessary.

The Classified Overlay column reflects the CNSSI 1253, Appendix F, Classified Overlay selection and identifies those security controls that must be applied to the baseline for all classified systems.

The Potentially Common/Inheritable column reflects those controls identified by CNSS as having a potential for implementation as a common control. The final determination as to whether a control is common (or hybrid) varies depending on the organization, mission, IS, and/or environment.

Any changes to the baseline security control selections must be addressed in the SCTM and must be approved by the Authorizing Official or designee (e.g., SCA).

ID	Title	C L	C M	C H	I L	I M	I H	A L	A M	A H	Classified Overlay	Potentially Common/ Inheritable
AC-1	Access Control Policy And Procedures	X	X	X	X	X	X	X	X	X		X
AC-2	Account Management	X	X	X	X	X	X					
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT		X	X		X	X					X
AC-2(2)	REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS		X	X		X	X					X

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
AC-2(3)	DISABLE INACTIVE ACCOUNTS		X	X		X	X					X
AC-2(4)	AUTOMATED AUDIT ACTIONS	X	X	X	X	X	X					X
AC-2(5)	INACTIVITY LOGOUT	X	X	X	X	X	X	X	X	X		X
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT											
AC-2(7)	ROLE-BASED SCHEMES	X	X	X	X	X	X					
AC-2(8)	DYNAMIC ACCOUNT CREATION											
AC-2(9)	RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS	X	X	X	X	X	X					X
AC-2(10)	SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION	X	X	X	X	X	X					
AC-2(11)	USAGE CONDITIONS			X			X					
AC-2(12)	ACCOUNT MONITORING / ATYPICAL USAGE	X	X	X	X	X	X					X
AC-2(13)	DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS	X	X	X	X	X	X					
AC-3	Access Enforcement	X	X	X	X	X	X					
AC-3(1)	*Withdrawn*											
AC-3(2)	DUAL AUTHORIZATION										+	
AC-3(3)	MANDATORY ACCESS CONTROL											
AC-3(4)	DISCRETIONARY ACCESS CONTROL	X	X	X	X	X	X				+	
AC-3(5)	SECURITY-RELEVANT INFORMATION											
AC-3(6)	*Withdrawn*											
AC-3(7)	ROLE-BASED ACCESS CONTROL											
AC-3(8)	REVOCATION OF ACCESS AUTHORIZATIONS											
AC-3(9)	CONTROLLED RELEASE											
AC-3(10)	AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS											
AC-4	Information Flow Enforcement		X	X		X	X					X
AC-4(1)	OBJECT SECURITY ATTRIBUTES											X
AC-4(2)	PROCESSING DOMAINS											X
AC-4(3)	DYNAMIC INFORMATION FLOW CONTROL											X
AC-4(4)	CONTENT CHECK ENCRYPTED INFORMATION											X
AC-4(5)	EMBEDDED DATA TYPES											X
AC-4(6)	METADATA											X
AC-4(7)	ONE-WAY FLOW MECHANISMS											X

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
AC-4(8)	SECURITY POLICY FILTERS											X
AC-4(9)	HUMAN REVIEWS											X
AC-4(10)	ENABLE / DISABLE SECURITY POLICY FILTERS											X
AC-4(11)	CONFIGURATION OF SECURITY POLICY FILTERS											X
AC-4(12)	DATA TYPE IDENTIFIERS											X
AC-4(13)	DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS											X
AC-4(14)	SECURITY POLICY FILTER CONSTRAINTS											X
AC-4(15)	DETECTION OF UNSANCTIONED INFORMATION											X
AC-4(16)	*Withdrawn*											
AC-4(17)	DOMAIN AUTHENTICATION											X
AC-4(18)	SECURITY ATTRIBUTE BINDING											
AC-4(19)	VALIDATION OF METADATA											X
AC-4(20)	APPROVED SOLUTIONS											X
AC-4(21)	PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS											X
AC-4(22)	ACCESS ONLY											X
AC-5	Separation Of Duties	X	X	X	X	X	X				+	
AC-6	Least Privilege	X	X	X	X	X	X				+	
AC-6(1)	AUTHORIZE ACCESS TO SECURITY FUNCTIONS	X	X	X	X	X	X					
AC-6(2)	NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	X	X	X	X	X	X					
AC-6(3)	NETWORK ACCESS TO PRIVILEGED COMMANDS			X			X					
AC-6(4)	SEPARATE PROCESSING DOMAINS											
AC-6(5)	PRIVILEGED ACCOUNTS	X	X	X	X	X	X					X
AC-6(6)	PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS											X
AC-6(7)	REVIEW OF USER PRIVILEGES	X	X	X	X	X	X				+	
AC-6(8)	PRIVILEGE LEVELS FOR CODE EXECUTION	X	X	X	X	X	X					
AC-6(9)	AUDITING USE OF PRIVILEGED FUNCTIONS	X	X	X	X	X	X					
AC-6(10)	PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	X	X	X	X	X	X					
AC-7	Unsuccessful Logon Attempts	X	X	X	X	X	X	X	X	X		
AC-7(1)	*Withdrawn*											

ID	Title	C L	C M	C H	I L	I M	I H	A L	A M	A H	Classified Overlay	Potentially Common/ Inheritable
AC-7(2)	PURGE / WIPE MOBILE DEVICE											
AC-8	System Use Notification	X	X	X	X	X	X					X
AC-9	Previous Logon (Access) Notification											
AC-9(1)	UNSUCCESSFUL LOGONS											
AC-9(2)	SUCCESSFUL / UNSUCCESSFUL LOGONS											
AC-9(3)	NOTIFICATION OF ACCOUNT CHANGES											
AC-9(4)	ADDITIONAL LOGON INFORMATION											
AC-10	Concurrent Session Control		X	X		X	X		X	X		
AC-11	Session Lock	X	X	X	X	X	X				+	
AC-11(1)	PATTERN-HIDING DISPLAYS	X	X	X							+	
AC-12	Session Termination		X	X		X	X					
AC-12(1)	USER-INITIATED LOGOUTS / MESSAGE DISPLAYS		X	X		X	X					
AC-13	*Withdrawn*											
AC-14	Permitted Actions Without Identification Or Authentication	X	X	X	X	X	X					
AC-14(1)	*Withdrawn*											
AC-15	*Withdrawn*											
AC-16	Security Attributes		X	X		X	X				+	
AC-16(1)	DYNAMIC ATTRIBUTE ASSOCIATION											
AC-16(2)	ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS											
AC-16(3)	MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM											
AC-16(4)	ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS											
AC-16(5)	ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES										+	
AC-16(6)	MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION		X	X		X	X				+	
AC-16(7)	CONSISTENT ATTRIBUTE INTERPRETATION										+	
AC-16(8)	ASSOCIATION TECHNIQUES / TECHNOLOGIES											
AC-16(9)	ATTRIBUTE REASSIGNMENT											
AC-16(10)	ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS											
AC-17	Remote Access	X	X	X	X	X	X					X

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
AC-17(1)	AUTOMATED MONITORING / CONTROL	X	X	X	X	X	X					X
AC-17(2)	PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION	X	X	X	X	X	X					X
AC-17(3)	MANAGED ACCESS CONTROL POINTS	X	X	X	X	X	X					X
AC-17(4)	PRIVILEGED COMMANDS / ACCESS	X	X	X	X	X	X					
AC-17(5)	*Withdrawn*											
AC-17(6)	PROTECTION OF INFORMATION	X	X	X								X
AC-17(7)	*Withdrawn*											
AC-17(8)	*Withdrawn*											
AC-17(9)	DISCONNECT / DISABLE ACCESS	X	X	X	X	X	X					X
AC-18	Wireless Access	X	X	X	X	X	X				+	X
AC-18(1)	AUTHENTICATION AND ENCRYPTION	X	X	X	X	X	X					X
AC-18(2)	*Withdrawn*											
AC-18(3)	DISABLE WIRELESS NETWORKING	X	X	X	X	X	X				+	X
AC-18(4)	RESTRICT CONFIGURATIONS BY USERS	X	X	X	X	X	X				+	X
AC-18(5)	ANTENNAS / TRANSMISSION POWER LEVELS			X			X					X
AC-19	Access Control For Mobile Devices	X	X	X	X	X	X				+	
AC-19(1)	*Withdrawn*											
AC-19(2)	*Withdrawn*											
AC-19(3)	*Withdrawn*											
AC-19(4)	RESTRICTIONS FOR CLASSIFIED INFORMATION											X
AC-19(5)	FULL DEVICE / CONTAINER-BASED ENCRYPTION		X	X		X	X					
AC-20	Use Of External Information Systems	X	X	X	X	X	X				+	X
AC-20(1)	LIMITS ON AUTHORIZED USE	X	X	X	X	X	X				+	X
AC-20(2)	PORTABLE STORAGE DEVICES	X	X	X							+	X
AC-20(3)	NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES	X	X	X	X	X	X				+	
AC-20(4)	NETWORK ACCESSIBLE STORAGE DEVICES										+	
AC-21	Information Sharing		X	X								
AC-21(1)	AUTOMATED DECISION SUPPORT											

ID	Title	C L	C M	C H	I L	I M	I H	A L	A M	A H	Classified Overlay	Potentially Common/ Inheritable
AC-21(2)	INFORMATION SEARCH AND RETRIEVAL											
AC-22	Publicly Accessible Content	X	X	X								X
AC-23	DATA MINING PROTECTION		X	X							+	X
AC-24	ACCESS CONTROL DECISIONS											
AC-24(1)	TRANSMIT ACCESS AUTHORIZATION INFORMATION											
AC-24(2)	NO USER OR PROCESS IDENTITY											
AC-25	REFERENCE MONITOR											
AT-1	Security Awareness And Training Policy And Procedures	X	X	X	X	X	X	X	X	X		X
AT-2	Security Awareness Training	X	X	X	X	X	X	X	X	X	+	X
AT-2(1)	PRACTICAL EXERCISES											X
AT-2(2)	INSIDER THREAT	X	X	X	X	X	X	X	X	X	+	X
AT-3	Role-Based Security Training	X	X	X	X	X	X	X	X	X		X
AT-3(1)	ENVIRONMENTAL CONTROLS											X
AT-3(2)	PHYSICAL SECURITY CONTROLS	X	X	X	X	X	X	X	X	X		X
AT-3(3)	PRACTICAL EXERCISES											X
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	X	X	X	X	X	X	X	X	X		X
AT-4	Security Training Records	X	X	X	X	X	X	X	X	X		X
AT-5	*Withdrawn*											
AU-1	Audit And Accountability Policy And Procedures	X	X	X	X	X	X	X	X	X		X
AU-2	Audit Events	X	X	X	X	X	X					
AU-2(1)	*Withdrawn*											
AU-2(2)	*Withdrawn*											
AU-2(3)	REVIEWS AND UPDATES	X	X	X	X	X	X					X
AU-2(4)	*Withdrawn*											
AU-3	Content Of Audit Records	X	X	X	X	X	X					
AU-3(1)	ADDITIONAL AUDIT INFORMATION	X	X	X	X	X	X					
AU-3(2)	CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT			X			X					X
AU-4	Audit Storage Capacity							X	X	X		
AU-4(1)	TRANSFER TO ALTERNATE STORAGE	X	X	X	X	X	X	X	X	X		
AU-5	Response To Audit Processing Failures							X	X	X		

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
AU-5(1)	AUDIT STORAGE CAPACITY							X	X	X		
AU-5(2)	REAL-TIME ALERTS									X		
AU-5(3)	CONFIGURABLE TRAFFIC VOLUME THRESHOLDS											
AU-5(4)	SHUTDOWN ON FAILURE											
AU-6	Audit Review, Analysis, And Reporting	X	X	X	X	X	X				+	X
AU-6(1)	PROCESS INTEGRATION	X	X	X	X	X	X					X
AU-6(2)	*Withdrawn*											
AU-6(3)	CORRELATE AUDIT REPOSITORIES	X	X	X	X	X	X					X
AU-6(4)	CENTRAL REVIEW AND ANALYSIS	X	X	X	X	X	X				+	
AU-6(5)	INTEGRATION / SCANNING AND MONITORING CAPABILITIES			X			X				+	X
AU-6(6)	CORRELATION WITH PHYSICAL MONITORING			X			X					X
AU-6(7)	PERMITTED ACTIONS											
AU-6(8)	FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS										+	
AU-6(9)	CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES										+	X
AU-6(10)	AUDIT LEVEL ADJUSTMENT	X	X	X	X	X	X					
AU-7	Audit Reduction And Report Generation		X	X		X	X					X
AU-7(1)	AUTOMATIC PROCESSING		X	X		X	X					X
AU-7(2)	AUTOMATIC SORT AND SEARCH											
AU-8	Time Stamps				X	X	X					
AU-8(1)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE				X	X	X					
AU-8(2)	SECONDARY AUTHORITATIVE TIME SOURCE											
AU-9	Protection Of Audit Information	X	X	X	X	X	X	X	X	X		
AU-9(1)	HARDWARE WRITE-ONCE MEDIA											
AU-9(2)	AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS									X		
AU-9(3)	CRYPTOGRAPHIC PROTECTION						X					
AU-9(4)	ACCESS BY SUBSET OF PRIVILEGED USERS	X	X	X	X	X	X					X
AU-9(5)	DUAL AUTHORIZATION											
AU-9(6)	READ ONLY ACCESS											

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
AU-10	Non-Repudiation					X	X					
AU-10(1)	ASSOCIATION OF IDENTITIES											
AU-10(2)	VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY											
AU-10(3)	CHAIN OF CUSTODY											
AU-10(4)	VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY											
AU-10(5)	*Withdrawn*											
AU-11	Audit Record Retention							X	X	X		X
AU-11(1)	LONG-TERM RETRIEVAL CAPABILITY							X	X	X		
AU-12	Audit Generation	X	X	X	X	X	X				+	
AU-12(1)	SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL				X	X	X					
AU-12(2)	STANDARDIZED FORMATS											
AU-12(3)	CHANGES BY AUTHORIZED INDIVIDUALS	X	X	X	X	X	X					
AU-13	Monitoring For Information Disclosure											X
AU-13(1)	USE OF AUTOMATED TOOLS											
AU-13(2)	REVIEW OF MONITORED SITES											
AU-14	Session Audit	X	X	X	X	X	X				+	
AU-14(1)	SYSTEM START-UP	X	X	X	X	X	X					
AU-14(2)	CAPTURE/RECORD AND LOG CONTENT	X	X	X	X	X	X					
AU-14(3)	REMOTE VIEWING / LISTENING	X	X	X								
AU-15	Alternate Audit Capability											
AU-16	Cross-Organizational Auditing										+	X
AU-16(1)	IDENTITY PRESERVATION										+	
AU-16(2)	SHARING OF AUDIT INFORMATION										+	
CA-1	Security Assessment And Authorization Policies And Procedures	X	X	X	X	X	X	X	X	X		X
CA-2	Security Assessments	X	X	X	X	X	X	X	X	X		X
CA-2(1)	INDEPENDENT ASSESSORS	X	X	X	X	X	X	X	X	X		X
CA-2(2)	SPECIALIZED ASSESSMENTS			X			X			X		X
CA-2(3)	EXTERNAL ORGANIZATIONS											X
CA-3	System Interconnections	X	X	X	X	X	X				+	
CA-3(1)	UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	X	X	X								X

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
CA-3(2)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS										+	X
CA-3(3)	UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS											
CA-3(4)	CONNECTIONS TO PUBLIC NETWORKS											
CA-3(5)	RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS	X	X	X	X	X	X					
CA-4	*Withdrawn*											
CA-5	Plan Of Action And Milestones	X	X	X	X	X	X	X	X	X		
CA-5(1)	AUTOMATION SUPPORT FOR ACCURACY / CURRENCY											
CA-6	Security Authorization	X	X	X	X	X	X	X	X	X		
CA-7	Continuous Monitoring	X	X	X	X	X	X	X	X	X		
CA-7(1)	INDEPENDENT ASSESSMENT		X	X		X	X		X	X		X
CA-7(2)	*Withdrawn*											
CA-7(3)	TREND ANALYSES											
CA-8	Penetration Testing						X					
CA-8(1)	INDEPENDENT PENETRATION AGENT OR TEAM											
CA-8(2)	RED TEAM EXERCISES											
CA-9	Internal System Connections	X	X	X	X	X	X					X
CA-9(1)	SECURITY COMPLIANCE CHECKS											
CM-1	Configuration Management Policy And Procedures	X	X	X	X	X	X					X
CM-2	Baseline Configuration				X	X	X					
CM-2(1)	REVIEWS AND UPDATES				X	X	X					X
CM-2(2)	AUTOMATION SUPPORT FOR ACCURACY / CURRENCY						X					
CM-2(3)	RETENTION OF PREVIOUS CONFIGURATIONS					X	X					
CM-2(4)	*Withdrawn*											
CM-2(5)	*Withdrawn*											
CM-2(6)	DEVELOPMENT AND TEST ENVIRONMENTS											
CM-2(7)	CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS					X	X					
CM-3	Configuration Change Control				X	X	X					X
CM-3(1)	AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES						X					X

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
CM-3(2)	TEST / VALIDATE / DOCUMENT CHANGES					X	X					
CM-3(3)	AUTOMATED CHANGE IMPLEMENTATION											
CM-3(4)	SECURITY REPRESENTATIVE				X	X	X					X
CM-3(5)	AUTOMATED SECURITY RESPONSE						X					
CM-3(6)	CRYPTOGRAPHY MANAGEMENT				X	X	X				+	
CM-4	Security Impact Analysis				X	X	X					X
CM-4(1)	SEPARATE TEST ENVIRONMENTS					X	X					
CM-4(2)	VERIFICATION OF SECURITY FUNCTIONS											
CM-5	Access Restrictions For Change				X	X	X					
CM-5(1)	AUTOMATED ACCESS ENFORCEMENT / AUDITING					X	X					
CM-5(2)	REVIEW SYSTEM CHANGES					X	X					
CM-5(3)	SIGNED COMPONENTS						X					
CM-5(4)	DUAL AUTHORIZATION											
CM-5(5)	LIMIT PRODUCTION / OPERATIONAL PRIVILEGES				X	X	X				+	X
CM-5(6)	LIMIT LIBRARY PRIVILEGES				X	X	X					X
CM-5(7)	*Withdrawn*											
CM-6	Configuration Settings				X	X	X					X
CM-6(1)	AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION					X	X					X
CM-6(2)	RESPOND TO UNAUTHORIZED CHANGES						X					
CM-6(3)	*Withdrawn*											
CM-6(4)	*Withdrawn*											
CM-7	Least Functionality	X	X	X	X	X	X					
CM-7(1)	PERIODIC REVIEW	X	X	X	X	X	X					
CM-7(2)	PREVENT PROGRAM EXECUTION	X	X	X	X	X	X					
CM-7(3)	REGISTRATION COMPLIANCE	X	X	X	X	X	X					X
CM-7(4)	UNAUTHORIZED SOFTWARE / BLACKLISTING											X
CM-7(5)	AUTHORIZED SOFTWARE / WHITELISTING	X	X	X	X	X	X					X
CM-8	Information System Component Inventory				X	X	X					X
CM-8(1)	UPDATES DURING INSTALLATIONS / REMOVALS					X	X					

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
CM-8(2)	AUTOMATED MAINTENANCE				X	X	X					X
CM-8(3)	AUTOMATED UNAUTHORIZED COMPONENT DETECTION				X	X	X					X
CM-8(4)	ACCOUNTABILITY INFORMATION			X			X					X
CM-8(5)	NO DUPLICATE ACCOUNTING OF COMPONENTS					X	X					X
CM-8(6)	ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS											X
CM-8(7)	CENTRALIZED REPOSITORY											X
CM-8(8)	AUTOMATED LOCATION TRACKING											X
CM-8(9)	ASSIGNMENT OF COMPONENTS TO SYSTEMS											X
CM-9	Configuration Management Plan				X	X	X					
CM-9(1)	ASSIGNMENT OF RESPONSIBILITY											X
CM-10	SOFTWARE USAGE RESTRICTIONS				X	X	X					X
CM-10(1)	OPEN SOURCE SOFTWARE				X	X	X					X
CM-11	USER-INSTALLED SOFTWARE	X	X	X	X	X	X					X
CM-11(1)	ALERTS FOR UNAUTHORIZED INSTALLATIONS			X			X					
CM-11(2)	PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS	X	X	X	X	X	X					
CP-1	Contingency Planning Policy And Procedures	X	X	X	X	X	X	X	X	X		X
CP-2	Contingency Plan							X	X	X		
CP-2(1)	COORDINATE WITH RELATED PLANS								X	X		
CP-2(2)	CAPACITY PLANNING									X		X
CP-2(3)	RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS								X	X		X
CP-2(4)	RESUME ALL MISSIONS / BUSINESS FUNCTIONS									X		X
CP-2(5)	CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS									X		X
CP-2(6)	ALTERNATE PROCESSING / STORAGE SITE											X
CP-2(7)	COORDINATE WITH EXTERNAL SERVICE PROVIDERS											
CP-2(8)	IDENTIFY CRITICAL ASSETS								X	X		
CP-3	Contingency Training							X	X	X		
CP-3(1)	SIMULATED EVENTS									X		

ID	Title	C L	C M	C H	I L	I M	I H	A L	A M	A H	Classified Overlay	Potentially Common/ Inheritable
CP-3(2)	AUTOMATED TRAINING ENVIRONMENTS											
CP-4	Contingency Plan Testing							X	X	X		
CP-4(1)	COORDINATE WITH RELATED PLANS								X	X		
CP-4(2)	ALTERNATE PROCESSING SITE									X		
CP-4(3)	AUTOMATED TESTING											
CP-4(4)	FULL RECOVERY / RECONSTITUTION											
CP-5	*Withdrawn*											
CP-6	Alternate Storage Site								X	X		X
CP-6(1)	SEPARATION FROM PRIMARY SITE								X	X		X
CP-6(2)	RECOVERY TIME / POINT OBJECTIVES									X		X
CP-6(3)	ACCESSIBILITY								X	X		X
CP-7	Alternate Processing Site		X	X		X	X		X	X		X
CP-7(1)	SEPARATION FROM PRIMARY SITE								X	X		X
CP-7(2)	ACCESSIBILITY								X	X		X
CP-7(3)	PRIORITY OF SERVICE								X	X		X
CP-7(4)	PREPARATION FOR USE									X		X
CP-7(5)	*Withdrawn*											
CP-7(6)	INABILITY TO RETURN TO PRIMARY SITE											X
CP-8	Telecommunications Services								X	X		X
CP-8(1)	PRIORITY OF SERVICE PROVISIONS								X	X		X
CP-8(2)	SINGLE POINTS OF FAILURE								X	X		X
CP-8(3)	SEPARATION OF PRIMARY / ALTERNATE PROVIDERS									X		X
CP-8(4)	PROVIDER CONTINGENCY PLAN									X		X
CP-8(5)	ALTERNATE TELECOMMUNICATION SERVICE TESTING									X		
CP-9	Information System Backup	X	X	X	X	X	X	X	X	X		
CP-9(1)	TESTING FOR RELIABILITY / INTEGRITY					X	X		X	X		
CP-9(2)	TEST RESTORATION USING SAMPLING									X		
CP-9(3)	SEPARATE STORAGE FOR CRITICAL INFORMATION									X		X
CP-9(4)	*Withdrawn*											

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
CP-9(5)	TRANSFER TO ALTERNATE STORAGE SITE								X	X		
CP-9(6)	REDUNDANT SECONDARY SYSTEM											
CP-9(7)	DUAL AUTHORIZATION											
CP-10	Information System Recovery And Reconstitution							X	X	X		X
CP-10(1)	*Withdrawn*											
CP-10(2)	TRANSACTION RECOVERY					X	X		X	X		
CP-10(3)	*Withdrawn*											
CP-10(4)	RESTORE WITHIN TIME PERIOD						X			X		
CP-10(5)	*Withdrawn*											
CP-10(6)	COMPONENT PROTECTION											
CP-11	Alternate Communications Protocols											
CP-12	Safe Mode											
CP-13	Alternative Security Mechanisms											
IA-1	Identification And Authentication Policy And Procedures	X	X	X	X	X	X					X
IA-2	Identification And Authentication (Organizational Users)	X	X	X	X	X	X				+	
IA-2(1)	NETWORK ACCESS TO PRIVILEGED ACCOUNTS	X	X	X	X	X	X				+	
IA-2(2)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS	X	X	X	X	X	X				+	
IA-2(3)	LOCAL ACCESS TO PRIVILEGED ACCOUNTS		X	X		X	X					
IA-2(4)	LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS		X	X		X	X					
IA-2(5)	GROUP AUTHENTICATION	X	X	X	X	X	X					
IA-2(6)	NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE											
IA-2(7)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE											
IA-2(8)	NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT	X	X	X	X	X	X					
IA-2(9)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT		X	X		X	X					
IA-2(10)	SINGLE SIGN-ON											
IA-2(11)	REMOTE ACCESS - SEPARATE DEVICE	X	X	X	X	X	X					
IA-2(12)	ACCEPTANCE OF PIV CREDENTIALS	X	X	X	X	X	X					

ID	Title	C L	C M	C H	I L	I M	I H	A L	A M	A H	Classified Overlay	Potentially Common/ Inheritable
IA-2(13)	OUT-OF-BAND AUTHENTICATION											
IA-3	Device Identification And Authentication	X	X	X	X	X	X					
IA-3(1)	CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION		X	X		X	X					
IA-3(2)	*Withdrawn*											
IA-3(3)	DYNAMIC ADDRESS ALLOCATION											X
IA-3(4)	DEVICE ATTESTATION											
IA-4	Identifier Management	X	X	X	X	X	X					X
IA-4(1)	PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS											
IA-4(2)	SUPERVISOR AUTHORIZATION											
IA-4(3)	MULTIPLE FORMS OF CERTIFICATION											
IA-4(4)	IDENTIFY USER STATUS	X	X	X	X	X	X					X
IA-4(5)	DYNAMIC MANAGEMENT											
IA-4(6)	CROSS-ORGANIZATION MANAGEMENT											
IA-4(7)	IN-PERSON REGISTRATION											
IA-5	Authenticator Management	X	X	X	X	X	X					X
IA-5(1)	PASSWORD-BASED AUTHENTICATION	X	X	X	X	X	X					
IA-5(2)	PKI-BASED AUTHENTICATION		X	X		X	X					
IA-5(3)	IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION					X	X					X
IA-5(4)	AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION	X	X	X	X	X	X					
IA-5(5)	CHANGE AUTHENTICATORS PRIOR TO DELIVERY											
IA-5(6)	PROTECTION OF AUTHENTICATORS											X
IA-5(7)	NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS	X	X	X								
IA-5(8)	MULTIPLE INFORMATION SYSTEM ACCOUNTS	X	X	X	X	X	X					X
IA-5(9)	CROSS-ORGANIZATION CREDENTIAL MANAGEMENT											
IA-5(10)	DYNAMIC CREDENTIAL ASSOCIATION											
IA-5(11)	HARDWARE TOKEN-BASED AUTHENTICATION				X	X	X					
IA-5(12)	BIOMETRIC AUTHENTICATION											

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
IA-5(13)	EXPIRATION OF CACHED AUTHENTICATORS	X	X	X	X	X	X					
IA-5(14)	MANAGING CONTENT OF PKI TRUST STORES	X	X	X	X	X	X					X
IA-5(15)	FICAM-APPROVED PRODUCTS AND SERVICES											
IA-6	Authenticator Feedback	X	X	X								
IA-7	Cryptographic Module Authentication	X	X	X	X	X	X					
IA-8	Identification And Authentication (Non-Organizational Users)	X	X	X	X	X	X					
IA-8(1)	ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES	X	X	X	X	X	X					
IA-8(2)	ACCEPTANCE OF THIRD-PARTY CREDENTIALS				X	X	X					
IA-8(3)	USE OF FICAM-APPROVED PRODUCTS				X	X	X					
IA-8(4)	USE OF FICAM-ISSUED PROFILES				X	X	X					
IA-8(5)	ACCEPTANCE OF PIV-I CREDENTIALS											
IA-9	Service Identification and Authentication											
IA-9(1)	INFORMATION EXCHANGE											
IA-9(2)	TRANSMISSION OF DECISIONS											
IA-10	Adaptive Identification and Authentication			X			X					
IA-11	Re-authentication			X			X					
IR-1	Incident Response Policy And Procedures	X	X	X	X	X	X	X	X	X		X
IR-2	Incident Response Training	X	X	X	X	X	X	X	X	X		
IR-2(1)	SIMULATED EVENTS			X			X			X		
IR-2(2)	AUTOMATED TRAINING ENVIRONMENTS						X			X		
IR-3	Incident Response Testing	X	X	X	X	X	X	X	X	X		
IR-3(1)	AUTOMATED TESTING											
IR-3(2)	COORDINATION WITH RELATED PLANS		X	X		X	X		X	X		
IR-4	Incident Handling	X	X	X	X	X	X	X	X	X		X
IR-4(1)	AUTOMATED INCIDENT HANDLING PROCESSES		X	X		X	X		X	X		X
IR-4(2)	DYNAMIC RECONFIGURATION											
IR-4(3)	CONTINUITY OF OPERATIONS		X	X		X	X		X	X		
IR-4(4)	INFORMATION CORRELATION	X	X	X	X	X	X	X	X	X		X

ID	Title	C L	C M	C H	I L	I M	I H	A L	A M	A H	Classified Overlay	Potentially Common/ Inheritable
IR-4(5)	AUTOMATIC DISABLING OF INFORMATION SYSTEM											
IR-4(6)	INSIDER THREATS - SPECIFIC CAPABILITIES	X	X	X	X	X	X	X	X	X		
IR-4(7)	INSIDER THREATS - INTRA-ORGANIZATION COORDINATION	X	X	X	X	X	X	X	X	X		
IR-4(8)	CORRELATION WITH EXTERNAL ORGANIZATIONS	X	X	X	X	X	X	X	X	X		
IR-4(9)	DYNAMIC RESPONSE CAPABILITY											
IR-4(10)	SUPPLY CHAIN COORDINATION											
IR-5	Incident Monitoring	X	X	X	X	X	X	X	X	X		X
IR-5(1)	AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS			X			X			X		X
IR-6	Incident Reporting	X	X	X	X	X	X	X	X	X		X
IR-6(1)	AUTOMATED REPORTING		X	X		X	X		X	X		X
IR-6(2)	VULNERABILITIES RELATED TO INCIDENTS	X	X	X	X	X	X	X	X	X		X
IR-6(3)	COORDINATION WITH SUPPLY CHAIN											
IR-7	Incident Response Assistance	X	X	X	X	X	X	X	X	X		X
IR-7(1)	AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT		X	X		X	X		X	X		X
IR-7(2)	COORDINATION WITH EXTERNAL PROVIDERS	X	X	X	X	X	X	X	X	X		X
IR-8	Incident Response Plan	X	X	X	X	X	X	X	X	X		X
IR-9	Information Spillage Response	X	X	X							+	
IR-9(1)	RESPONSIBLE PERSONNEL	X	X	X							+	
IR-9(2)	TRAINING	X	X	X							+	
IR-9(3)	POST-SPILL OPERATIONS								X	X		
IR-9(4)	EXPOSURE TO UNAUTHORIZED PERSONNEL	X	X	X							+	
IR-10	Integrated Information Security Cell		X	X		X	X		X	X		
MA-1	System Maintenance Policy And Procedures	X	X	X	X	X	X	X	X	X		X
MA-2	Controlled Maintenance	X	X	X	X	X	X	X	X	X		
MA-2(1)	*Withdrawn*											
MA-2(2)	AUTOMATED MAINTENANCE ACTIVITIES			X			X			X		
MA-3	Maintenance Tools				X	X	X					X
MA-3(1)	INSPECT TOOLS					X	X					X
MA-3(2)	INSPECT MEDIA				X	X	X					X
MA-3(3)	PREVENT UNAUTHORIZED REMOVAL	X	X	X							+	

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
MA-3(4)	RESTRICTED TOOL USE											
MA-4	Nonlocal Maintenance				X	X	X					
MA-4(1)	AUDITING AND REVIEW					X	X					X
MA-4(2)	DOCUMENT NONLOCAL MAINTENANCE					X	X					
MA-4(3)	COMPARABLE SECURITY / SANITIZATION	X	X	X	X	X	X					
MA-4(4)	AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS											
MA-4(5)	APPROVALS AND NOTIFICATIONS											X
MA-4(6)	CRYPTOGRAPHIC PROTECTION	X	X	X	X	X	X					
MA-4(7)	REMOTE DISCONNECT VERIFICATION				X	X	X					
MA-5	Maintenance Personnel	X	X	X	X	X	X	X	X	X		
MA-5(1)	INDIVIDUALS WITHOUT APPROPRIATE ACCESS			X			X			X	+	
MA-5(2)	SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS											X
MA-5(3)	CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS											X
MA-5(4)	FOREIGN NATIONALS											
MA-5(5)	NONSYSTEM-RELATED MAINTENANCE											
MA-6	Timely Maintenance								X	X		
MA-6(1)	PREVENTIVE MAINTENANCE											
MA-6(2)	PREDICTIVE MAINTENANCE											
MA-6(3)	AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE											
MP-1	Media Protection Policy And Procedures	X	X	X	X	X	X				+	X
MP-2	Media Access	X	X	X	X	X	X				+	X
MP-2(1)	*Withdrawn*											
MP-2(2)	*Withdrawn*											
MP-3	Media Marking		X	X							+	
MP-4	Media Storage		X	X		X	X				+	
MP-4(1)	*Withdrawn*											
MP-4(2)	AUTOMATED RESTRICTED ACCESS											
MP-5	Media Transport		X	X		X	X				+	X
MP-5(1)	*Withdrawn*											
MP-5(2)	*Withdrawn*											
MP-5(3)	CUSTODIANS										+	X
MP-5(4)	CRYPTOGRAPHIC PROTECTION		X	X		X	X				+	

ID	Title	C L	C M	C H	I L	I M	I H	A L	A M	A H	Classified Overlay	Potentially Common/ Inheritable
MP-6	Media Sanitization	X	X	X							+	X
MP-6(1)	REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY			X							+	X
MP-6(2)	EQUIPMENT TESTING			X							+	X
MP-6(3)	NONDESTRUCTIVE TECHNIQUES			X							+	
MP-6(4)	*Withdrawn*											
MP-6(5)	*Withdrawn*											
MP-6(6)	*Withdrawn*											
MP-6(7)	DUAL AUTHORIZATION											
MP-6(8)	REMOTE PURGING / WIPING OF INFORMATION											
MP-7	Media Use	X	X	X	X	X	X				+	
MP-7(1)	PROHIBIT USE WITHOUT OWNER				X	X	X					
MP-7(2)	PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA											
MP-8	Media Downgrading										+	
MP-8(1)	DOCUMENTATION OF PROCESS										+	
MP-8(2)	EQUIPMENT TESTING										+	
MP-8(3)	CONTROLLED UNCLASSIFIED INFORMATION											
MP-8(4)	CLASSIFIED INFORMATION										+	
PE-1	Physical And Environmental Protection Policy And Procedures	X	X	X	X	X	X	X	X	X		X
PE-2	Physical Access Authorizations	X	X	X	X	X	X	X	X	X		X
PE-2(1)	ACCESS BY POSITION / ROLE											X
PE-2(2)	TWO FORMS OF IDENTIFICATION											
PE-2(3)	RESTRICT UNESCORTED ACCESS										+	X
PE-3	Physical Access Control	X	X	X	X	X	X	X	X	X		X
PE-3(1)	INFORMATION SYSTEM ACCESS	X	X	X	X	X	X					X
PE-3(2)	FACILITY / INFORMATION SYSTEM BOUNDARIES										+	X
PE-3(3)	CONTINUOUS GUARDS / ALARMS / MONITORING										+	X
PE-3(4)	LOCKABLE CASINGS											
PE-3(5)	TAMPER PROTECTION											
PE-3(6)	FACILITY PENETRATION TESTING											X
PE-4	Access Control For Transmission Medium		X	X		X	X				+	X

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
PE-5	Access Control For Output Devices		X	X								
PE-5(1)	ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS											
PE-5(2)	ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY											
PE-5(3)	MARKING OUTPUT DEVICES										+	
PE-6	Monitoring Physical Access	X	X	X	X	X	X	X	X	X		
PE-6(1)	INTRUSION ALARMS / SURVEILLANCE EQUIPMENT		X	X		X	X		X	X		
PE-6(2)	AUTOMATED INTRUSION RECOGNITION / RESPONSES											
PE-6(3)	VIDEO SURVEILLANCE											
PE-6(4)	MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS			X			X			X		
PE-7	*Withdrawn*											
PE-7(1)	*Withdrawn*											
PE-7(2)	*Withdrawn*											
PE-8	Visitor Access Records	X	X	X	X	X	X	X	X	X		X
PE-8(1)	AUTOMATED RECORDS MAINTENANCE / REVIEW			X			X					
PE-8(2)	*Withdrawn*											
PE-9	Power Equipment And Cabling								X	X		X
PE-9(1)	REDUNDANT CABLING											
PE-9(2)	AUTOMATIC VOLTAGE CONTROLS											X
PE-10	Emergency Shutoff								X	X		X
PE-10(1)	*Withdrawn*											
PE-11	Emergency Power								X	X		
PE-11(1)	LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY									X		X
PE-11(2)	LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED											X
PE-12	Emergency Lighting							X	X	X		X
PE-12(1)	ESSENTIAL MISSIONS / BUSINESS FUNCTIONS											X
PE-13	Fire Protection							X	X	X		X
PE-13(1)	DETECTION DEVICES / SYSTEMS									X		X
PE-13(2)	SUPPRESSION DEVICES / SYSTEMS									X		X
PE-13(3)	AUTOMATIC FIRE SUPPRESSION								X	X		X

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
PE-13(4)	INSPECTIONS									X		X
PE-14	Temperature And Humidity Controls							X	X	X		X
PE-14(1)	AUTOMATIC CONTROLS											X
PE-14(2)	MONITORING WITH ALARMS / NOTIFICATIONS											X
PE-15	Water Damage Protection							X	X	X		X
PE-15(1)	AUTOMATION SUPPORT									X		
PE-16	Delivery And Removal	X	X	X	X	X	X	X	X	X		X
PE-17	Alternate Work Site		X	X		X	X		X	X		
PE-18	Location Of Information System Components									X		X
PE-18(1)	FACILITY SITE											X
PE-19	Information Leakage										+	
PE-19(1)	NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES										+	
PE-20	ASSET MONITORING AND TRACKING											
PL-1	Security Planning Policy And Procedures	X	X	X	X	X	X	X	X	X		X
PL-2	System Security Plan	X	X	X	X	X	X	X	X	X		
PL-2(1)	*Withdrawn*											
PL-2(2)	*Withdrawn*											
PL-2(3)	PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES		X	X		X	X		X	X		
PL-3	*Withdrawn*											
PL-4	Rules Of Behavior	X	X	X	X	X	X	X	X	X		
PL-4(1)	SOCIAL MEDIA AND NETWORKING RESTRICTIONS		X	X								X
PL-5	*Withdrawn*											
PL-6	*Withdrawn*											
PL-7	Security Concept Of Operations											
PL-8	Information Security Architecture	X	X	X	X	X	X	X	X	X		
PL-8(1)	DEFENSE-IN-DEPTH	X	X	X	X	X	X	X	X	X		
PL-8(2)	SUPPLIER DIVERSITY	X	X	X	X	X	X	X	X	X		
PL-9	Central Management											X
PS-1	Personnel Security Policy And Procedures	X	X	X	X	X	X	X	X	X		X
PS-2	Position Risk Designation	X	X	X	X	X	X	X	X	X		X
PS-3	Personnel Screening	X	X	X	X	X	X					
PS-3(1)	CLASSIFIED INFORMATION										+	
PS-3(2)	FORMAL INDOCTRINATION	S	S	S								

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
PS-3(3)	INFORMATION WITH SPECIAL PROTECTION MEASURES											
PS-4	Personnel Termination	X	X	X	X	X	X	X	X	X	+	
PS-4(1)	POST-EMPLOYMENT REQUIREMENTS	X	X	X							+	
PS-4(2)	AUTOMATED NOTIFICATION			X			X			X		
PS-5	Personnel Transfer	X	X	X	X	X	X	X	X	X		
PS-6	Access Agreements	X	X	X	X	X	X					X
PS-6(1)	*Withdrawn*											
PS-6(2)	CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION										+	X
PS-6(3)	POST-EMPLOYMENT REQUIREMENTS	X	X	X							+	
PS-7	Third-Party Personnel Security	X	X	X	X	X	X					X
PS-8	Personnel Sanctions	X	X	X	X	X	X	X	X	X		X
RA-1	Risk Assessment Policy And Procedures	X	X	X	X	X	X	X	X	X		X
RA-2	Security Categorization	X	X	X	X	X	X	X	X	X		
RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X		
RA-4	*Withdrawn*											
RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X		
RA-5(1)	UPDATE TOOL CAPABILITY	X	X	X	X	X	X	X	X	X		
RA-5(2)	UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED	X	X	X	X	X	X	X	X	X		
RA-5(3)	BREADTH / DEPTH OF COVERAGE											X
RA-5(4)	DISCOVERABLE INFORMATION	X	X	X	X	X	X	X	X	X		
RA-5(5)	PRIVILEGED ACCESS	X	X	X	X	X	X	X	X	X		
RA-5(6)	AUTOMATED TREND ANALYSES											
RA-5(7)	*Withdrawn*											
RA-5(8)	REVIEW HISTORIC AUDIT LOGS											
RA-5(9)	*Withdrawn*											
RA-5(10)	CORRELATE SCANNING INFORMATION			X			X			X		
RA-6	Technical Surveillance Countermeasures Survey										+	
SA-1	System And Services Acquisition Policy And Procedures	X	X	X	X	X	X	X	X	X		X
SA-2	Allocation Of Resources	X	X	X	X	X	X	X	X	X		
SA-3	System Development Life Cycle	X	X	X	X	X	X	X	X	X		
SA-4	Acquisition Process	X	X	X	X	X	X	X	X	X		

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
SA-4(1)	FUNCTIONAL PROPERTIES OF SECURITY CONTROLS		X	X		X	X		X	X		X
SA-4(2)	DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS		X	X		X	X		X	X		X
SA-4(3)	DEVELOPMENT METHODS / TECHNIQUES / PRACTICES						X					X
SA-4(4)	*Withdrawn*											
SA-4(5)	SYSTEM / COMPONENT / SERVICE CONFIGURATIONS						X					X
SA-4(6)	USE OF INFORMATION ASSURANCE PRODUCTS										+	X
SA-4(7)	NIAP-APPROVED PROTECTION PROFILES				X	X	X					
SA-4(8)	CONTINUOUS MONITORING PLAN											
SA-4(9)	FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE	X	X	X	X	X	X	X	X	X		
SA-4(10)	USE OF APPROVED PIV PRODUCTS	X	X	X	X	X	X					
SA-5	Information System Documentation	X	X	X	X	X	X	X	X	X		
SA-5(1)	*Withdrawn*											
SA-5(2)	*Withdrawn*											
SA-5(3)	*Withdrawn*											
SA-5(4)	*Withdrawn*											
SA-5(5)	*Withdrawn*											
SA-6	*Withdrawn*											
SA-6(1)	*Withdrawn*											
SA-7	*Withdrawn*											
SA-8	Security Engineering Principles	X	X	X	X	X	X	X	X	X		X
SA-9	External Information System Services	X	X	X	X	X	X	X	X	X		
SA-9(1)	RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS				X	X	X					X
SA-9(2)	IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES	X	X	X	X	X	X	X	X	X		
SA-9(3)	ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS											
SA-9(4)	CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS											
SA-9(5)	PROCESSING, STORAGE, AND SERVICE LOCATION											
SA-10	Developer Configuration Management				X	X	X					

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
SA-10(1)	SOFTWARE / FIRMWARE INTEGRITY VERIFICATION				X	X	X					
SA-10(2)	ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES											
SA-10(3)	HARDWARE INTEGRITY VERIFICATION											
SA-10(4)	TRUSTED GENERATION											
SA-10(5)	MAPPING INTEGRITY FOR VERSION CONTROL											
SA-10(6)	TRUSTED DISTRIBUTION											
SA-11	Developer Security Testing and Evaluation		X	X		X	X		X	X		
SA-11(1)	STATIC CODE ANALYSIS											
SA-11(2)	THREAT AND VULNERABILITY ANALYSES											
SA-11(3)	INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE											
SA-11(4)	MANUAL CODE REVIEWS											
SA-11(5)	PENETRATION TESTING / ANALYSIS											
SA-11(6)	ATTACK SURFACE REVIEWS											
SA-11(7)	VERIFY SCOPE OF TESTING / EVALUATION											
SA-11(8)	DYNAMIC CODE ANALYSIS											
SA-12	Supply Chain Protection	X	X	X	X	X	X	X	X	X		X
SA-12(1)	ACQUISITION STRATEGIES / TOOLS / METHODS			X			X			X		
SA-12(2)	SUPPLIER REVIEWS											X
SA-12(3)	*Withdrawn*											
SA-12(4)	*Withdrawn*											
SA-12(5)	LIMITATION OF HARM			X			X			X		
SA-12(6)	*Withdrawn*											
SA-12(7)	ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE											
SA-12(8)	USE OF ALL-SOURCE INTELLIGENCE			X			X			X		
SA-12(9)	OPERATIONS SECURITY			X			X			X		
SA-12(10)	VALIDATE AS GENUINE AND NOT ALTERED											
SA-12(11)	PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS			X			X			X		
SA-12(12)	INTER-ORGANIZATIONAL AGREEMENTS											

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
SA-12(13)	CRITICAL INFORMATION SYSTEM COMPONENTS											
SA-12(14)	IDENTITY AND TRACEABILITY											
SA-12(15)	PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES											
SA-13	Trustworthiness											
SA-14	Criticality Analysis			X			X			X		
SA-14(1)	*Withdrawn*											
SA-15	Development Process, Standards, And Tools	X	X	X	X	X	X	X	X	X		
SA-15(1)	QUALITY METRICS											
SA-15(2)	SECURITY TRACKING TOOLS											
SA-15(3)	CRITICALITY ANALYSIS			X			X			X		
SA-15(4)	THREAT MODELING / VULNERABILITY ANALYSIS			X			X			X		
SA-15(5)	ATTACK SURFACE REDUCTION											
SA-15(6)	CONTINUOUS IMPROVEMENT											
SA-15(7)	AUTOMATED VULNERABILITY ANALYSIS						X					
SA-15(8)	REUSE OF THREAT / VULNERABILITY INFORMATION											
SA-15(9)	USE OF LIVE DATA	X	X	X							+	
SA-15(10)	INCIDENT RESPONSE PLAN											
SA-15(11)	ARCHIVE INFORMATION SYSTEM / COMPONENT											
SA-16	Developer Provided Training			X			X			X		
SA-17	Developer Security Architecture And Design			X			X			X		
SA-17(1)	FORMAL POLICY MODEL											
SA-17(2)	SECURITY-RELEVANT COMPONENTS											
SA-17(3)	FORMAL CORRESPONDENCE											
SA-17(4)	INFORMAL CORRESPONDENCE											
SA-17(5)	CONCEPTUALLY SIMPLE DESIGN											
SA-17(6)	STRUCTURE FOR TESTING											
SA-17(7)	STRUCTURE FOR LEAST PRIVILEGE											
SA-18	Tamper Resistance And Detection											
SA-18(1)	MULTIPLE PHASES OF SDLC											
SA-18(2)	INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES											
SA-19	Component Authenticity				X	X	X					

ID	Title	C L	C M	C H	I L	I M	I H	A L	A M	A H	Classified Overlay	Potentially Common/ Inheritable
SA-19(1)	ANTI-COUNTERFEIT TRAINING											
SA-19(2)	CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR											
SA-19(3)	COMPONENT DISPOSAL											
SA-19(4)	ANTI-COUNTERFEIT TRAINING											
SA-20	Customized Development Of Critical Components											
SA-21	DEVELOPER SCREENING											
SA-21(1)	VALIDATION OF SCREENING											
SA-22	Unsupported System Components	S	S	X	S	S	X	S	S	X		
SA-22(1)	ALTERNATIVE SOURCES FOR CONTINUED SUPPORT											
SC-1	System And Communications Protection Policy And Procedures	X	X	X	X	X	X	X	X	X		X
SC-2	Application Partitioning		X	X		X	X				+	
SC-2(1)	INTERFACES FOR NON-PRIVILEGED USERS											
SC-3	Security Function Isolation			X			X				+	X
SC-3(1)	HARDWARE SEPARATION											
SC-3(2)	ACCESS / FLOW CONTROL FUNCTIONS											
SC-3(3)	MINIMIZE NONSECURITY FUNCTIONALITY											
SC-3(4)	MODULE COUPLING AND COHESIVENESS											
SC-3(5)	LAYERED STRUCTURES											
SC-4	Information In Shared Resources		X	X								
SC-4(1)	*Withdrawn*											
SC-4(2)	PERIODS PROCESSING											
SC-5	Denial Of Service Protection							X	X	X		
SC-5(1)	RESTRICT INTERNAL USERS							X	X	X		
SC-5(2)	EXCESS CAPACITY / BANDWIDTH / REDUNDANCY								X	X		
SC-5(3)	DETECTION / MONITORING								X	X		
SC-6	Resource Availability											
SC-7	Boundary Protection	X	X	X	X	X	X					X
SC-7(1)	*Withdrawn*											
SC-7(2)	*Withdrawn*											
SC-7(3)	ACCESS POINTS	X	X	X	X	X	X					
SC-7(4)	EXTERNAL TELECOMMUNICATIONS SERVICES	X	X	X	X	X	X					
SC-7(5)	DENY BY DEFAULT / ALLOW BY EXCEPTION	X	X	X	X	X	X					

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
SC-7(6)	*Withdrawn*											
SC-7(7)	PREVENT SPLIT TUNNELING FOR REMOTE DEVICES	X	X	X	X	X	X					
SC-7(8)	ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS	X	X	X	X	X	X					X
SC-7(9)	RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC				X	X	X					
SC-7(10)	PREVENT UNAUTHORIZED EXFILTRATION	X	X	X								
SC-7(11)	RESTRICT INCOMING COMMUNICATIONS TRAFFIC				X	X	X					
SC-7(12)	HOST-BASED PROTECTION	X	X	X	X	X	X	X	X	X		
SC-7(13)	ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS	X	X	X	X	X	X					X
SC-7(14)	PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS	X	X	X	X	X	X					
SC-7(15)	ROUTE PRIVILEGED NETWORK ACCESSES											
SC-7(16)	PREVENT DISCOVERY OF COMPONENTS / DEVICES											
SC-7(17)	AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS											
SC-7(18)	FAIL SECURE			X			X			X		
SC-7(19)	BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS											
SC-7(20)	DYNAMIC ISOLATION / SEGREGATION											
SC-7(21)	ISOLATION OF INFORMATION SYSTEM COMPONENTS			X			X					
SC-7(22)	SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS											
SC-7(23)	DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE											
SC-8	Transmission Confidentiality And Integrity	X	X	X	X	X	X				+	
SC-8(1)	CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION	X	X	X	X	X	X				+	
SC-8(2)	PRE / POST TRANSMISSION HANDLING		X	X		X	X					

ID	Title	C L	C M	C H	I L	I M	I H	A L	A M	A H	Classified Overlay	Potentially Common/ Inheritable
SC-8(3)	CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS										+	
SC-8(4)	CONCEAL / RANDOMIZE COMMUNICATIONS										+	
SC-9	*Withdrawn*											
SC-9(1)	*Withdrawn*											
SC-9(2)	*Withdrawn*											
SC-10	Network Disconnect		X	X		X	X					
SC-11	Trusted Path											
SC-11(1)	LOGICAL ISOLATION											
SC-12	Cryptographic Key Establishment And Management	X	X	X	X	X	X					X
SC-12(1)	AVAILABILITY							S	S	X		
SC-12(2)	SYMMETRIC KEYS										+	
SC-12(3)	ASYMMETRIC KEYS										+	
SC-12(4)	*Withdrawn*											
SC-12(5)	*Withdrawn*											
SC-13	Cryptographic Protection	X	X	X	X	X	X				+	
SC-13(1)	*Withdrawn*											
SC-13(2)	*Withdrawn*											
SC-13(3)	*Withdrawn*											
SC-13(4)	*Withdrawn*											
SC-14	*Withdrawn*											
SC-15	Collaborative Computing Devices	X	X	X								
SC-15(1)	PHYSICAL DISCONNECT											
SC-15(2)	*Withdrawn*											
SC-15(3)	DISABLING / REMOVAL IN SECURE WORK AREAS										+	
SC-15(4)	EXPLICITLY INDICATE CURRENT PARTICIPANTS											
SC-16	Transmission Of Security Attributes											
SC-16(1)	INTEGRITY VALIDATION											
SC-17	Public Key Infrastructure Certificates	X	X	X	X	X	X					X
SC-18	Mobile Code				X	X	X					X
SC-18(1)	IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS				X	X	X					X
SC-18(2)	ACQUISITION / DEVELOPMENT / USE				X	X	X					X
SC-18(3)	PREVENT DOWNLOADING / EXECUTION				X	X	X					
SC-18(4)	PREVENT AUTOMATIC EXECUTION				X	X	X					
SC-18(5)	ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS											X

ID	Title	C L	C M	C H	I L	I M	I H	A L	A M	A H	Classified Overlay	Potentially Common/ Inheritable
SC-19	Voice Over Internet Protocol	X	X	X	X	X	X	X	X	X		X
SC-20	Secure Name / Address Resolution Service (Authoritative Source)				X	X	X					
SC-20(1)	*Withdrawn*											
SC-20(2)	DATA ORIGIN / INTEGRITY											
SC-21	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)				X	X	X					
SC-21(1)	*Withdrawn*											
SC-22	Architecture And Provisioning For Name / Address Resolution Service	X	X	X	X	X	X	X	X	X		
SC-23	Session Authenticity				X	X	X					
SC-23(1)	INVALIDATE SESSION IDENTIFIERS AT LOGOUT				X	X	X					
SC-23(2)	*Withdrawn*											
SC-23(3)	UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION				X	X	X					
SC-23(4)	*Withdrawn*											
SC-23(5)	ALLOWED CERTIFICATE AUTHORITIES				X	X	X					
SC-24	Fail In Known State			X			X					
SC-25	Thin Nodes											
SC-26	Honeypots											
SC-26(1)	*Withdrawn*											
SC-27	Platform-Independent Applications											
SC-28	Protection Of Information At Rest	X	X	X	X	X	X				+	
SC-28(1)	CRYPTOGRAPHIC PROTECTION	X	X	X	X	X	X				+	
SC-28(2)	OFF-LINE STORAGE											
SC-29	Heterogeneity											
SC-29(1)	VIRTUALIZATION TECHNIQUES											
SC-30	Concealment and Misdirection											
SC-30(1)	*Withdrawn*											
SC-30(2)	RANDOMNESS											
SC-30(3)	CHANGE PROCESSING / STORAGE LOCATIONS											
SC-30(4)	MISLEADING INFORMATION											
SC-30(5)	CONCEALMENT OF SYSTEM COMPONENTS											
SC-31	Covert Channel Analysis											
SC-31(1)	TEST COVERT CHANNELS FOR EXPLOITABILITY											
SC-31(2)	MAXIMUM BANDWIDTH											
SC-31(3)	MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS											

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
SC-32	Information System Partitioning											
SC-33	*Withdrawn*											
SC-34	Non-Modifiable Executable Programs											
SC-34(1)	NO WRITABLE STORAGE											
SC-34(2)	INTEGRITY PROTECTION / READ-ONLY MEDIA											
SC-34(3)	HARDWARE-BASED PROTECTION											
SC-35	Honeyclients											
SC-36	Distributed Processing And Storage											
SC-36(1)	POLLING TECHNIQUES											
SC-37	Out-Of-Band Channels											
SC-37(1)	ENSURE DELIVERY / TRANSMISSION											
SC-38	Operations Security	X	X	X	X	X	X	X	X	X		
SC-39	Process Isolation	X	X	X	X	X	X					
SC-39(1)	HARDWARE SEPARATION											
SC-39(2)	THREAD ISOLATION											
SC-40	Wireless Link Protection											
SC-40(1)	ELECTROMAGNETIC INTERFERENCE											
SC-40(2)	REDUCE DETECTION POTENTIAL											
SC-40(3)	IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION											
SC-40(4)	SIGNAL PARAMETER IDENTIFICATION											
SC-41	Port And I/O Device Access											
SC-42	Sensor Capability And Data										+	
SC-42(1)	REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES											
SC-42(2)	AUTHORIZED USE											
SC-42(3)	PROHIBIT USE OF DEVICES										+	
SC-43	Usage Restrictions											X
SC-44	Detonation Chambers											
SI-1	System And Information Integrity Policy And Procedures	X	X	X	X	X	X	X	X	X		X
SI-2	Flaw Remediation				X	X	X					X
SI-2(1)	CENTRAL MANAGEMENT				X	X	X					
SI-2(2)	AUTOMATED FLAW REMEDIATION STATUS				X	X	X					
SI-2(3)	TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS				X	X	X					X

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
SI-2(4)	*Withdrawn*											
SI-2(5)	AUTOMATIC SOFTWARE / FIRMWARE UPDATES											
SI-2(6)	REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE				X	X	X					
SI-3	Malicious Code Protection				X	X	X					X
SI-3(1)	CENTRAL MANAGEMENT				X	X	X					X
SI-3(2)	AUTOMATIC UPDATES				X	X	X					
SI-3(3)	*Withdrawn*											
SI-3(4)	UPDATES ONLY BY PRIVILEGED USERS											
SI-3(5)	*Withdrawn*											
SI-3(6)	TESTING / VERIFICATION											
SI-3(7)	NONSIGNATURE-BASED DETECTION											
SI-3(8)	DETECT UNAUTHORIZED COMMANDS											
SI-3(9)	AUTHENTICATE REMOTE COMMANDS											
SI-3(10)	MALICIOUS CODE ANALYSIS				X	X	X					
SI-4	Information System Monitoring	X	X	X	X	X	X	X	X	X		
SI-4(1)	SYSTEM-WIDE INTRUSION DETECTION SYSTEM	X	X	X	X	X	X	X	X	X		
SI-4(2)	AUTOMATED TOOLS FOR REAL-TIME ANALYSIS		X	X		X	X		X	X		
SI-4(3)	AUTOMATED TOOL INTEGRATION											
SI-4(4)	INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	X	X	X	X	X	X	X	X	X		
SI-4(5)	SYSTEM-GENERATED ALERTS	X	X	X	X	X	X	X	X	X		
SI-4(6)	*Withdrawn*											
SI-4(7)	AUTOMATED RESPONSE TO SUSPICIOUS EVENTS											
SI-4(8)												
SI-4(9)	TESTING OF MONITORING TOOLS											
SI-4(10)	VISIBILITY OF ENCRYPTED COMMUNICATIONS		X	X		X	X		X	X		X
SI-4(11)	ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES	X	X	X	X	X	X	X	X	X		
SI-4(12)	AUTOMATED ALERTS	X	X	X	X	X	X	X	X	X		
SI-4(13)	ANALYZE TRAFFIC / EVENT PATTERNS											
SI-4(14)	WIRELESS INTRUSION DETECTION	X	X	X	X	X	X	X	X	X	+	

ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
SI-4(15)	WIRELESS TO WIRELINE COMMUNICATIONS	X	X	X	X	X	X	X	X	X		
SI-4(16)	CORRELATE MONITORING INFORMATION	X	X	X	X	X	X	X	X	X		
SI-4(17)	INTEGRATED SITUATIONAL AWARENESS											X
SI-4(18)	ANALYZE TRAFFIC / COVERT EXFILTRATION											
SI-4(19)	INDIVIDUALS POSING GREATER RISK	X	X	X	X	X	X	X	X	X	+	
SI-4(20)	PRIVILEGED USER	X	X	X	X	X	X	X	X	X		
SI-4(21)	PROBATIONARY PERIODS										+	
SI-4(22)	UNAUTHORIZED NETWORK SERVICES	X	X	X	X	X	X	X	X	X		
SI-4(23)	HOST-BASED DEVICES	X	X	X	X	X	X	X	X	X		
SI-4(24)	INDICATORS OF COMPROMISE											
SI-5	Security Alerts, Advisories, And Directives				X	X	X					X
SI-5(1)	AUTOMATED ALERTS AND ADVISORIES						X					X
SI-6	Security Function Verification						X					
SI-6(1)	*Withdrawn*											
SI-6(2)	AUTOMATION SUPPORT FOR DISTRIBUTED TESTING											
SI-6(3)	REPORT VERIFICATION RESULTS						X					X
SI-7	Software Firmware, And Information Integrity					X	X					X
SI-7(1)	INTEGRITY CHECKS					X	X					
SI-7(2)	AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS						X					
SI-7(3)	CENTRALLY-MANAGED INTEGRITY TOOLS											
SI-7(4)	*Withdrawn*											
SI-7(5)	AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS						X					
SI-7(6)	CRYPTOGRAPHIC PROTECTION											
SI-7(7)	INTEGRATION OF DETECTION AND RESPONSE					X	X					
SI-7(8)	AUDITING CAPABILITY FOR SIGNIFICANT EVENTS					X	X					
SI-7(9)	VERIFY BOOT PROCESS											
SI-7(10)	PROTECTION OF BOOT FIRMWARE											
SI-7(11)	CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES											

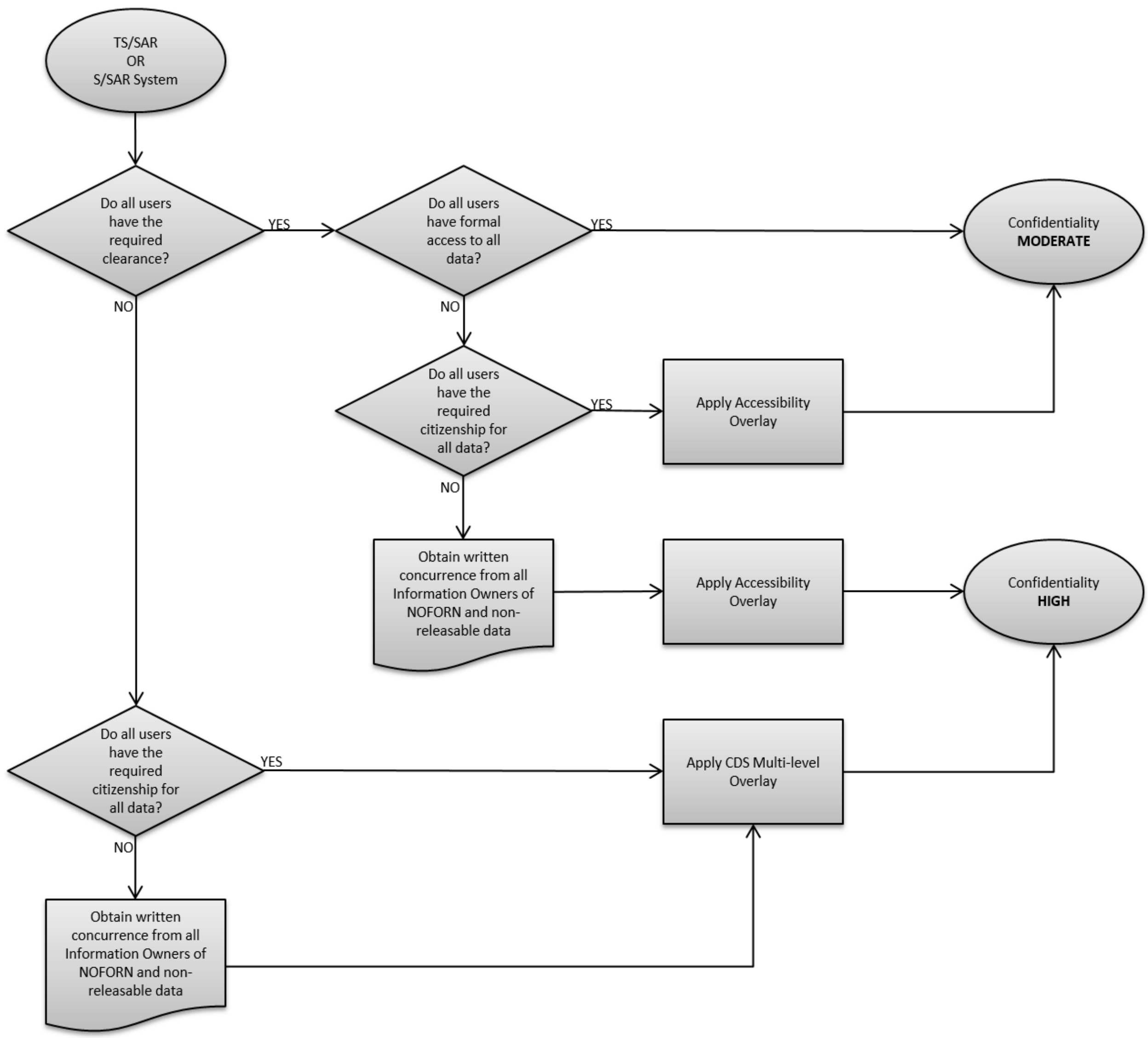
ID	Title	C	C	C	I	I	I	A	A	A	Classified Overlay	Potentially Common/ Inheritable
		L	M	H	L	M	H	L	M	H		
SI-7(12)	INTEGRITY VERIFICATION											
SI-7(13)	CODE EXECUTION IN PROTECTED ENVIRONMENTS											
SI-7(14)	BINARY OR MACHINE EXECUTABLE CODE				X *	X	X					
SI-7(15)	CODE AUTHENTICATION											
SI-7(16)	TIME LIMIT ON PROCESS EXECUTION W/O SUPERVISION											
SI-8	Spam Protection					X	X		X	X		X
SI-8(1)	CENTRAL MANAGEMENT					X	X		X	X		X
SI-8(2)	AUTOMATIC UPDATES					X	X		X	X		
SI-8(3)	CONTINUOUS LEARNING CAPABILITY											
SI-9	*Withdrawn*											
SI-10	Information Input Validation				X	X	X					
SI-10(1)	MANUAL OVERRIDE CAPABILITY											
SI-10(2)	REVIEW / RESOLUTION OF ERRORS											
SI-10(3)	PREDICTABLE BEHAVIOR					X	X					
SI-10(4)	REVIEW / TIMING INTERACTIONS											
SI-10(5)	REVIEW/RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS											
SI-11	Error Handling				X	X	X					
SI-12	Information Handling And Retention	X	X	X	X	X	X					X
SI-13	Predictable Failure Prevention											
SI-13(1)	TRANSFERRING COMPONENT RESPONSIBILITIES											
SI-13(2)	*Withdrawn*											
SI-13(3)	MANUAL TRANSFER BETWEEN COMPONENTS											
SI-13(4)	STANDBY COMPONENT INSTALLATION / NOTIFICATION											
SI-13(5)	FAILOVER CAPABILITY											
SI-14	Non-Persistence											
SI-14(1)	REFRESH FROM TRUSTED SOURCES											
SI-15	Information Output Filtering											
SI-16	Memory Protection					X	X					
SI-17	Fail-Safe Procedures											
PM-1	Information Security Program Plan	X	X	X	X	X	X	X	X	X		
PM-2	Senior Information Security Officer	X	X	X	X	X	X	X	X	X		
PM-3	Information Security Resources	X	X	X	X	X	X	X	X	X		

ID	Title	C L	C M	C H	I L	I M	I H	A L	A M	A H	Classified Overlay	Potentially Common/ Inheritable
PM-4	Plan of Action and Milestones Process	X	X	X	X	X	X	X	X	X	CNSSI 1253: PM controls are common controls deployed organization-wide, supporting an information security program.	
PM-5	Information System Inventory	X	X	X	X	X	X	X	X	X		
PM-6	Information Security Measures of Performance	X	X	X	X	X	X	X	X	X		
PM-7	Enterprise Architecture	X	X	X	X	X	X	X	X	X		
PM-8	Critical Infrastructure Plan	X	X	X	X	X	X	X	X	X		
PM-9	Risk Management Strategy	X	X	X	X	X	X	X	X	X		
PM-10	Security Authorization Process	X	X	X	X	X	X	X	X	X		
PM-11	Mission/Business Process Definition	X	X	X	X	X	X	X	X	X		
PM-12	Insider Threat Program	X	X	X	X	X	X	X	X	X		
PM-13	Information Security Workforce	X	X	X	X	X	X	X	X	X		
PM-14	Testing, Training, and Monitoring	X	X	X	X	X	X	X	X	X		
PM-15	Contacts With Security Groups And Associations	X	X	X	X	X	X	X	X	X		
PM-16	Threat Awareness Program	X	X	X	X	X	X	X	X	X		
AP-1	Authority To Collect											
AP-2	Purpose Specification											
AR-1	Governance And Privacy Program											
AR-2	Privacy Impact And Risk Assessment											
AR-3	Privacy Requirements For Contractors And Service Providers											
AR-4	Privacy Monitoring And Auditing											
AR-5	Privacy Awareness And Training											
AR-6	Privacy Reporting											
AR-7	Privacy-Enhanced System Design And Development											
AR-8	Accounting Of Disclosures											
DI-1	Data Quality											
DI-1(1)	VALIDATE PII											
DI-1(2)	RE-VALIDATE PII											
DI-2	Data Integrity And Data Integrity Board											
DI-2(1)	PUBLISH AGREEMENTS ON WEBSITE											
DM-1	Minimization Of Personally Identifiable Information											
DM-1(1)	LOCATE / REMOVE / REDACT / ANONYMIZE PII											
DM-2	Data Retention And Disposal											
DM-2(1)	SYSTEM CONFIGURATION											
DM-3	Minimization Of PII Used In Testing, Training, And Research											
DM-3(1)	RISK MINIMIZATION TECHNIQUES											

ID	Title	C L	C M	C H	I L	I M	I H	A L	A M	A H	Classified Overlay	Potentially Common/ Inheritable
IP-1	Consent											
IP-1(1)	MECHANISMS SUPPORTING ITEMIZED OR TIERED CONSENT											
IP-2	Individual Access											
IP-3	Redress											
IP-4	Complaint Management											
IP-4(1)	RESPONSE TIMES											
SE-1	Inventory Of Personally Identifiable Information											
SE-2	Privacy Incident Response											
TR-1	Privacy Notice											
TR-1(1)	REAL-TIME OR LAYERED NOTICE											
TR-2	System Of Records Notices And Privacy Act Statements											
TR-2(1)	PUBLIC WEBSITE PUBLICATION											
TR-3	Dissemination Of Privacy Program Information											
UL-1	Internal Use											
UL-2	Information Sharing With Third Parties											

* SI-7(14) - Consider tailoring out if not implementing the base control, SI-7

APPENDIX D: Confidentiality Impact Level Flowchart



APPENDIX E: Definitions

Application	Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. [CNSSI 4009]
Clearing	Clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. In general, laboratory techniques allow the retrieval of information that has been cleared, but normal operations do not allow such retrieval.
Closed Source Software (CSS)	Also known as Proprietary software.
Commercial off-the-Shelf (COTS) Software	Copyrighted or open source vendor software publicly available for purchase.
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]
Cross Domain Solution (CDS)	A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. [CNSSI 4009]
Data Spill or Classified Information Spillage	Classified data is spilled either onto an unclassified information system or to an information system with a lower [or different] level of classification [or access]. [CNSSI 4009] Also referred to as data exfiltration – the unauthorized transfer of data from a system.
Denial of Service (DoS) or Distributed Denial of Service (DDoS)	The prevention of authorized access to resources or the delaying of time-critical operations. DDoS is a technique that uses numerous hosts to perform the attack. [CNSSI 4009]
Event	Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. [CNSSI 4009]
Freeware	Copyrighted software given away for free by the author. Although it is available for free, the author retains the copyright and does not distribute source code, so other people cannot market the software as their own.
Government off-the-Shelf (GOTS) Software	Software developed with government funds for government use.
Incident	An assessed occurrence that actually or potentially jeopardizes the confidentially, integrity or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.[CNSSI 4009]
Initial Denial Authority	An official granted authority by the head of a DoD Component to withhold records requested under the Freedom of Information Act.
Intellectual Property	Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract properties has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered.[CNSSI-4009]

Local Area Network (LAN)	A group of computers and network devices connected together over a relatively small geographic area. A LAN may be isolated – no connections outside the system boundary or facility; or interconnected to another system or LAN.
Mobile Device	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). [NIST SP 800-53 Rev4] See also Portable Electronic Device (PED).
Nonce	A time-varying value that has at most a negligible chance of repeating, for example, a random value that is generated anew for each use, a timestamp, a sequence number, or some combination of these. [NIST SP 800-102] [See also CNSSI 4009 definition]
Non-persistent Information	Any information not authorized to be stored within a facility, both digital and non-digital. This includes ensuring that information systems resident to a facility do not retain data locally after session termination beyond what the facility is approved for. [See PE-1]
Open Source Software (OSS)	The 16 October 2009 memorandum from the DoD CIO, "Clarifying Guidance Regarding Open Source Software (OSS)" defines OSS is defined as “software for which the human-readable source code is available for use, study, re-use, modification, enhancement, and redistribution by the users of that software.” The program source code is generally developed as a community in which programmers improve upon the code and share the changes. See http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx for more details.
Organization	Within this document the entity identified as ‘organization’ varies. It refers to that element (government unit or company) to which the ISO belongs unless handled at a higher echelon.
Portable Electronic Device (PED)	Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, video cameras, and pagers.[CNSSI 4009]
Platform Information Technology (PIT)	Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. [DoD 8500.01E; DoDI 8580.1] Note: Do not choose this definition unless your system is designated as a PIT.
Public Domain Software	Software not protected by copyright laws of any nation that may be freely used without permission of, or payment to, the creator, and that carries no warranties from, or liabilities to the creator. [CNSSI 4009]

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 Discretionary access Control (DAC), Mandatory Access Control (MAC), Network Access Control (NAC).
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.
Security Supporting	Impacts a security process or procedures: e.g., software used to perform technical review for Assured File Transfer (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.
Shareware	Software distributed on the basis of an honor system. Most shareware is delivered free of charge, but the author usually requests that the user pay a small fee if they continue to use the program. By sending the small fee, the user is registered with the producer who in turn provides assistance and updates. Shareware is inexpensive because it is usually produced by a single programmer and is offered directly to customers. Thus, there is practically no packaging or advertising expenses. Note that shareware differs from public-domain software in that shareware is copyrighted and source code is not made available. This means that the user cannot sell a shareware product as his/her own.
Standalone	A standalone IS may include desktop, laptop, and notebook personal computers, and any other hand-held electronic device containing classified information. Standalone IS by definition are not connected to any LAN or other type of network, i.e., peripherals allowed, but no network interface card (NIC) in use, no protected distribution system (PDS) in place, no additional computers connected.
State of the Practice	The highest level of development at a particular time (especially the present time; e.g., current incident response tools/techniques; current intrusion detection tools, techniques, procedures).
System Types	Examples include: LAN, WAN, standalone, CI, CDS, PIT, application
Unattended IS Components	Discovery of unlocked active session without user present.
Unattended Processing	Automated processes executed/running on a user's behalf while no users are physically present in the area/facility.
Unauthorized Access	Any access that violates the stated security policy. [CNSSI 4009]
Unauthorized Disclosure	An event involving the exposure of information to entities not authorized access to the information. [CNSSI 4009]
Unauthorized Monitoring	Any monitoring of an IS without written approval from security authorities.
Unauthorized Software	Software obtained through unofficial channels and installed without proper approval.
Wide Area Network (WAN)	Computer network that spans a relatively large geographical area.