U.S. Department of Homeland Security

DHS Policy Directive

Number: 4300A

Version 13.3
Issue Date: February 13, 2023

Information Technology System Security Program, Sensitive Systems

---

KENNETH W BIBLE

Digitally signed by KENNETH W BIBLE
Date: 2023.05.23 13:16:10 -04'00'

Kenneth Bible
Chief Information Security Officer

Date

DOCUMENT CHANGE HISTORY

Issue	Date	Pages Affected	Description
13.2	August 22, 2022	All	This version rewritten around the NIST SP 800-53, Revision 5 Control Families, all instructions, procedures and SOP non-applicable policy statements moved to the attachment documents, authorities updated, and comments adjudicated and implemented from the Policy Working Group and all participating component representatives (Barbara Brough, Risk Management and Compliance , Assessments Branch)
13.3	February 13, 2023	18, 23	This version updated to revise retention requirements and add new section regarding risk acceptances that can be approved by the Component CIO/CISO.

TABLE OF CONTENTS

1) Introduction

Organizations depend on information systems to carry out their missions and business functions. The success of the mission and business functions depends on protecting the confidentiality, integrity, and availability of information processed, stored, and transmitted by those systems. The threats to information systems include equipment failure, environmental disruptions, human or machine errors, and purposeful attacks that are often sophisticated, disciplined, well-organized, and well-funded. When successful, attacks on information systems can result in serious or catastrophic damage to organizational operations and assets, individuals, other organizations, and the Nation. Therefore, it is imperative that organizations remain vigilant, and that senior executives, leaders, and managers understand their responsibilities and are accountable for protecting organizational assets and for managing risk.

The E-Government Act of 2002 (Public Law 107-347) recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) of 2002, requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security that supports the operations of the agency, including those provided or managed by another agency, contractor, or other source. The Federal Information Security Modernization Act (FISMA) of 2014 amended the FISMA of 2002, providing several modifications that modernize federal security and privacy practices to address evolving security concerns. One of these changes is to emphasize risk-based policy standards for federal information and information systems for cost-effective security and privacy.

The Presidential Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017) and (EO) 14028 *Improving the Nation's Cybersecurity (May 21, 2021)* also outlined actions to enhance cybersecurity across federal agencies and critical infrastructure partners, and reinforces FISMA 2014.

The Department of Homeland Security (DHS) Information Security Program lays the foundation for DHS security personnel to implement and maintain secure DHS information system design, operation, and maintenance. Information security policy makes certain assumptions about protection measures that respond to other DHS security policies and practices (e.g., physical and personnel security). For example, this policy presupposes reliable processes for confirming the credentials of prospective system users. Information security policy also presumes the enforcement of suitable physical protection from the means of access to facilities storing DHS's IT resources.

The requirements of this policy complement other agency measures for effective management of assets and regulatory compliance (e.g., with the federal privacy laws). References

are made to those sources throughout this document (latest version published is referenced). As the primary information source for fundamental requirements for maintaining the confidentiality, integrity, and availability of information technology (IT) resources, the policy identifies and characterizes a comprehensive set of basic protection goals without stipulating how the goals should be met (i.e., the specific technologies, mechanisms, or procedures involved).

2) Information System Security Program

The DHS Information System Security Program, Sensitive Systems, provides a baseline of policies, procedures, standards, and guidelines for DHS Components. This Policy Directive provides direction to managers and senior leadership on how to manage and protect sensitive systems. It also defines policies relating to managerial, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, authenticity, and nonrepudiation in DHS information system infrastructure and operations. The policy elements expressed in this Directive are designed to be broad in scope to accommodate diverse operating environments. Each DHS Component is responsible for the identification, development, and implementation of any additional policies needed to meet their specific requirements. Implementation information can often be found in specific National Institute of Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

This Policy Directive pertains to DHS Sensitive Systems, as distinct from the DHS National Security Systems (NSS), which are governed by the DHS National Security Systems Policy Directive 4300B series[1]. The 4300B policy series applies to all DHS elements, employees, contractors, detailees, others working on behalf of DHS, and users of DHS NSS that collect, generate, process, store, display, transmit, or receive Unclassified, Confidential, Secret, Top Secret (TS), or Special Access Program (SAP) National Security Information (NSI). Please see DHS Management Directive 140-01, "*Information Technology System Security Program*" for additional detail.

Policy elements are effective when issued. Failure to implement any policy element within 135 days of discovery is considered a weakness, and either a system or program Plan of Action and Milestones (POA&M) is generated by the Component for the identified weaknesses within 145 days from discovery and submitted to the FISMA repository. When this Policy Directive is changed, the DHS Chief Information Officer (CIO), via the Chief Information Security Officer (CISO), will ensure that appropriate tool changes are made available to the Department within 90 days of the policy change.

[1] National Security Cyber Division (dhs.gov)

3) Purpose

This DHS Policy Directive 4300A, *"Information Technology System Security Program, Sensitive Systems,"* hereafter known as DHS 4300A, establishes the information security policy for DHS. This program is based on federal security regulations and highlights DHS's goals and requirements for protecting its' information and information system assets. This program prescribes responsibilities, practices, and conditions that directly or indirectly promote security in the development, operation, maintenance, and support of all DHS IT resources. This program also identifies security practices that align with DHS's mission, provides cost-effective protection of DHS's information and information systems, and responds to security and privacy issues associated with contemporary technologies and risks. This program is aligned with current and applicable federal security laws, policies, and regulations.

This program is intended to provide protection goals and standards by providing a comprehensive view of information security and privacy considerations to all DHS Components, personnel, and information systems. It addresses technical security services, as well as the management and operational requirements for information security. This program identifies all relevant security and privacy roles and responsibilities, as well as affected organizations. This program also reflects the increasing requirements needed for internal and external security oversight from the DHS Office of Inspector General (OIG) and for responding to FISMA requirements.

The scope of this policy is as follows:

a) The policy statements in the DHS 4300A, in alignment with NIST SP 800-53, Revision 5, address security and privacy controls in the *DHS Control Baseline*s which apply to low, moderate, and high impact systems. See Attachment CC, the *DHS Security and Privacy Control Baseline with Operationally Defined Values (ODV)*, hereafter known as the *DHS Control Baseline*, for additional details. DISA Security Technical Implementation Guides, or STIGs, are used as configuration checklists referring to the DHS Baseline and used as both a Configuration checklist and assessment guide as a part of the control implementation and validation process.
b) The Cybersecurity Framework (CSF) Subcategories[i] (or controls) are not within the scope of this policy. However, the CSF Subcategories are mapped to the controls within each control family in the Security and Privacy Control Catalog to provide a better overview of the control family.

4) Rescission

This policy supersedes the DHS 4300A Sensitive Systems Policy and Sensitive

Systems Policy Handbook. See authorities for additional memos, directives, and policies included in this document.

5) Applicability

The DHS 4300A is intended to serve a diverse audience within DHS, including:

a) Individuals with system, information security, privacy, or risk management and oversight responsibilities.
b) Employees, contractors, and service providers with system development responsibilities including, for example, system owners, program managers, systems engineers, systems security engineers, privacy engineers, software developers, systems integrators, and acquisition or procurement officials.
c) Employees, contractors, and service providers with security and privacy implementation and operations responsibilities including, for example, Program Offices, mission or business owners, system owners, information owners or stewards, system administrators/engineers, network engineers, system security or privacy officers.
d) Employees, contractors, and service providers with security and privacy assessment and monitoring responsibilities including, for example, auditors, Inspectors General, system evaluators, control assessors, independent verifiers and validators, and analysts.
e) Users of DHS information systems, including employees, contractors, and members of the general public, especially users of these systems who are not information security professionals and have a limited understanding of the complexities of threats facing DHS systems. The DHS Information Security Program must support users by providing systems that accomplish security objectives in a manner that provides for the continued utility and usability of these systems.

6) Effective Implementation Date

The authority for the issuance of this policy rests with the CIO and is assigned to the DHS Chief Information Security Office Directorate (CISOD). DHS CISOD serves as the central focal point for cybersecurity within DHS. This DHS Information Security Program is effective in accordance with the established timeline for transition and implementation approved by the CISO Council.

This Policy Directive will be reviewed annually from the date of issuance to assess its effectiveness and update as necessary, when implementation challenges arise, or when impacted by a significant change or underlying standard. For example, the potential use of

newer technologies (e.g., wireless communications) may give rise to additional policy requirements. In such cases, the policy will outline the basic relevant security and privacy policy requirements; however, in general, the policy is free from low-level procedural and technical detail.

All updates to this Policy Directive shall be subject to the DHS-wide clearance process providing an opportunity for stakeholders to comment on the subject matter and content of the directive, such as on the implication of programmatic implementation of the proposed updates.

7) Policy

DHS information security and privacy policies are based on Federal Information Security Modernization Act of 2014 (FISMA 2014) and the Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016). This policy document integrates the security and privacy requirements from the Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, and controls that are documented in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations (December 2020)*, with DHS-specific requirements.

This Policy Directive is intended to simplify compliance with current versions of FIPS 200 and NIST SP 800-53, Revision 5, which is the basis of the DHS Control Baseline and Organizational Defined Values (ODV). See Attachment CC of this Policy Directive *DHS Baselines and ODVs* for additional detail. This Policy Directive is organized by NIST security and privacy control families. Each new control family has an overview and description of the family followed by high-level policy statements.

Policy Overview

DHS information security policies define the security management structure and foundation needed to ensure adequate control over DHS sensitive information and systems.

Authorities

The following are authoritative references for the DHS Sensitive Information Security Program. Additional references are located in the Authorities and References section of this Directive.

- E-Government Act of 2002, Public Law 107–347, 116 Stat. 2899, 44 U.S.C. 101
- Federal Information Security Modernization Act of 2014 (FISMA), Public Law

113- 283; 128 Stat 3073

- Cybersecurity Information Sharing Act of 2015.
- Office of Management and Budget (OMB) Circular A- 123 "Managing Information as a Strategic Resource," July 2016.
- DHS Management Directive 140-01 "Information Technology System Security Program."
- National Institute of Standards and Technology (NIST) Federal Information Processing Standard FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006.
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," December 2020.
- NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations," December 2018.

(AC) Access Control Family

Access control is a method of guaranteeing that users are who they say they are and that they have the authorized access to the data being sought. At a high level, access control is a selective restriction of access to data. Access control addresses user authorization to utilize an information system. It also addresses the processes and types of transactions that are allowed. Who should access DHS's data? How does DHS ensure those who attempted access have unequivocally been granted that access? Under which circumstances do you deny access to a user with access privileges?

To effectively protect its data, DHS's access control policy must address these questions. Information system access must be limited to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). This promotes the least functionality paradigm by giving people, processes, or devices the most basic functionality required for completing tasks as a basic user or a privileged account holder.

DHS's access control requirements, at a minimum, shall:

1. Employ at the component level, a centralized identity management system for user accounts, including:

    a) Suspend accounts for personnel on extended absences, as defined by Human Resources

    b) Employ a process to record and monitor significant changes to user accounts and groups to ensure access is not granted outside the formal DHS approval process

    c) Create and assign administrator accounts separate from normal user accounts for individuals requiring escalated privileges.

    d) Ensure system owners review information system accounts supporting their programs at least annually and when major changes occur to the systems environments.

    e) Ensure separation of duties to prevent abuse of authorized privileges and help to reduce the risk of malevolent activity without collusion.

    f) Employ least privilege for job roles on DHS information systems to ensure that the processes operate at privilege levels no higher than necessary to accomplish required DHS missions/business functions. Develop policy for the use of password managers (e.g. LastPass, CyberArk, cloud based solutions such as Azure Active Directory, etc.,)

2. For DHS employees that leverage internal or external resources that use passwords for access control. See NIST SP 800-63 for additional password guidelines.

3. Enable the use of Multifactor Authentication as outlined in Homeland Security Presidential Directive (HSPD)-12 which mandates a federal standard for secure and reliable forms of identification [e.g., Personal Identity Verification (PIV) Card].

    a) Components shall provide phishing-resistant authentication methods (e.g., FIDO2, Web Authentication) for its systems. See NIST 800-63b for additional details.

    b) Components shall provide phishing-resistant authentication methods for public-facing systems that support multi-factor authentication.

4. Develop a policy on data exchange and interconnection security agreements (ISAs) for all DHS systems connected to external systems. Ensure prevention of unauthorized access to DHS information systems and networks. See FIPS 199 and NIST 800-171 for requirements.

5. Ensure DHS Components develop and document access agreements for information systems and ensure that individuals requiring access to information and information systems sign access agreements, prior to being granted access. Access agreements must be re-signed, by all parties, when agreements have been updated. Access agreements are reviewed at least

annually.

6. Ensure that DHS Components train users on rules of behavior and that each user signs a rules of behavior agreement within 5 business days of first accessing a DHS system

7. Ensure that wireless mobile devices are not tethered or otherwise physically or wirelessly connected to the DHS-wired core network, without the prior written consent of the Authorizing Official (AO). For additional requirement details see NIST SP 800-124, Revision 2 (DRAFT), "Guidelines for Managing the Security of Mobile Devices in the Enterprise," March 2020 and NIST SP 800-121 Revision 2, "Guide to Bluetooth Security," May 2020.

    a) Ensure that pairings are made only between approved (Bluetooth, wireless, mobile, etc.) devices.

    b) Disable Bluetooth functionality when not in use. See NIST SP 800-121 Rev. 2, "Guide to Bluetooth Security" for additional requirement details.

    c) Ensure that devices are configured for manual pairing and prompt the user to authorize any incoming connection requests; auto pairing may not be implemented.

    d) Maintain devices in non-discoverable mode, except during device pairing.

    e) Pair devices to receivers, in personally owned vehicles, for voice communication as approved by the AO.

    f) Ensure that devices use low power to minimize the range of communication.

8. Ensure DHS Components identify and implement appropriate operational and technical controls to limit unauthorized tracking or targeting of radio-frequency identification (RFID)-tagged items, when these items are expected to travel outside of the Component's physical perimeter.

9. Employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. See NIST SP 800-77, Revision 1, "*Guide to IPsec VPNs*," June 2020.

10. Ensure that multiple or split tunnel communication paths are not enabled on devices except where authorized using the Trusted Internet Connection (TIC) 3.0 modernization guidance, Split Tunneling can allow trusted applications to be split from the VPN tunnel, and managed by the Cloud Access Security Broker, with the management of the connection for compliance control managed by the broker at the management point.

11. Ensure that Personally Identifiable Information (PII), law enforcement sensitive information, and security sensitive information complies with all DHS requirements for sensitive systems, including strong authentication. Strong authentication is accomplished by means of VPN or equivalent encryption and two-factor authentication. The risk assessment and security plans (SP) must document any remote access of PII, and the approval of remote access is approved by the DHS Authorizing Official (AO) prior to implementation. " See FIPS 140-2, FIPS 140-

3, NIST SP 800-53, Revision 5, and NIST SP 800-63.

a) Additionally, remote access of Personally Identifiable Information (PII), law enforcement sensitive information, and security sensitive information does not permit the download and remote storage of information unless the requirements for the use of removable media with sensitive information have been addressed. All downloads follow the concept of least privilege and are documented in the Security Plan (SP). See FIPS 199 and NIST 800-53 Revision 5 as a part of the DHS security baseline, Attachment CC of this document.

12. Shall display a warning banner, specified by the DHS CISOD, for all internal DHS systems.

a) Provide security and privacy statements, at every entry point, for systems accessible to the public.

b) Concur that the use of DHS information systems by any user (including DHS personnel, contractors, and others working on behalf of DHS) is subject to monitoring or search at any time. By completing the authentication process, the user acknowledges their consent to monitoring and acknowledges that they have no expectation of privacy for their use of or for information stored in such systems.

c) Concur that the use of Government office equipment and DHS systems/computers constitutes consent to monitoring and auditing, of the equipment/systems at all times. Monitoring includes the tracking of internal transactions and external transactions such as Internet access. It also includes auditing of stored data on local and network storage devices as well as removable media.

(AT) Awareness and Training Control Family

All levels of DHS management must ensure employees, contractors, vendors, and other third-party entities are informed of their security responsibilities and the need to attain required continued education relevant to information security, their position within DHS, and their Program Offices. Maintaining a level of due diligence, ensures that key objectives of an effective Information Security Program are attained. All employees and contractors must understand their roles and responsibilities and become adequately trained to perform them, thus, ensuring the protection of the confidentiality, integrity, and availability of DHS information systems and the information they contain.

All DHS users and personnel, including contractors, who leverage DHS information Systems have a responsibility to consider their responsibilities for any system they access and be aware of all security risks associated with their use and management of that system. Mechanisms must be established to verify and track security awareness and specialized security training for personnel who have been designated as having significant security responsibilities (i.e., Federal Workforce Assessment surveys).

DHS's awareness and training requirements, at a minimum, shall:

AT 1: Cybersecurity Awareness and Training Program

1. Components must establish a Cybersecurity Awareness and Training Program for users of DHS information systems.2. Components prepare and submit a Cybersecurity Awareness and Training Annual Implementation Plan (to include role-based training) each fiscal year to the DHS Enterprise Cybersecurity Awareness and Training Program by the end of the first quarter.

2. The DHS CISO will provide oversight of Component Cybersecurity Awareness and Training Program Plans and Component Cybersecurity Awareness and Training Annual Implementation Plans. The DHS CISO will review both plans annually.

3. Components prepare and submit ad hoc cybersecurity awareness reports with content, frequency, format, and distribution at the request of the DHS CISO.

AT 2: Initial Basic and Annual Refresher Cybersecurity Awareness Training

1. DHS personnel, contractors, or others working on behalf of DHS (i.e., employees, detailees, military) accessing DHS systems will receive Initial Basic Cybersecurity Awareness Training which, at a minimum, must cover basic cybersecurity literacy and concepts, terms, threats, and rules for using a system(s). Personnel must complete Initial Basic Cybersecurity Awareness Training within 5 business days of first accessing a DHS system. Components will take appropriate actions, up to and including suspension of the user account, to ensure training completion.

2. DHS personnel, contractors, or others working on behalf of DHS (i.e., employees, detailees, military) accessing DHS systems will receive Annual Refresher Cybersecurity Awareness Training (CSAT) in security awareness and accepted security practices. If Annual Refresher Cybersecurity Awareness Training is not completed, Components will take appropriate actions, up to and including suspension of the user account, to ensure training completion. Components shall have the flexibility to determine whether annual refresher CSAT completion will be tracked based on fiscal year or calendar year.

3. Components must maintain sufficient Initial Basic and Annual Refresher Cybersecurity Awareness Training records as produced by the Component's Learning Management System (LMS), to include compliant and non-compliant CSAT users. Records must be maintained in accordance with Office of the Chief Human Capital Officer (OCHCO) or National Archives and Records Administration (NARA) training records retention requirements.

4. User accounts and access privileges, including access to email, is temporarily disabled for those DHS employees who have not completed Annual Refresher Cybersecurity Awareness Training, unless a waiver is granted by the Component's Chief Information Security Officer (CISO) or Information Systems Security Manager (ISSM). The account will only be re-enabled to allow the user to complete the CSAT module and course completion will be verified in the LMS.

5. Components must provide CSAT (Initial Basic CSAT and Annual Refresher CSAT) training

completion statistics by April 30th, July 31st, and October 1st to the Enterprise Cybersecurity Awareness and Training Program using the designated format.

AT 3: Role-based Training

1. DHS personnel, contractors, or others working on behalf of DHS (i.e., employees, detailees, military) with significant cybersecurity responsibilities must receive specialized training as defined in NIST SP 800-181 or DHS minimum role-based standards prior to obtaining access to the system(s) containing sensitive information. Examples of minimum roles include: Information Systems Security Officers (ISSO), Information Systems Security Managers (ISSM), Authorizing Official (AO), System Owners (SO), System Administrators, etc.). Individuals designated as having a role with significant cybersecurity responsibility must complete refresher training each fiscal year, thereafter.
   Primary role-based training will be based on the NIST SP 800-181 requirements, followed by DHS specific training requirements for roles with significant cybersecurity responsibility.

2. Components must maintain sufficient Role-based Training records as produced by the Component's Learning Management System (LMS), to include compliant and non-compliant users. Records must be maintained in accordance with Office of the Chief Human Capital Officer (OCHCO) or National Archives and Records Administration (NARA) training records retention requirements.

3. Components must provide role-based training completion statistics by April 30th and October 1st to the Enterprise Cybersecurity Awareness and Training Program using the designated format.

Privacy

1. DHS Components will administer basic privacy training annually and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII annually. See the *(PT) Personally Identifiable Information Processing and Transparency Control Family for additional details.*

2. Ensure managers and users of DHS information systems are made aware of the security and privacy risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, and procedures related to the security of DHS information systems.

3. Components develop, implement, and update a comprehensive Privacy training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.

4. DHS Components ensure that personnel annually certify (manually or electronically) acceptance of responsibilities for privacy requirements.

Rules of Behavior & General Information

1. Ensure that DHS Components train users on rules of behavior and that each user signs a rules of behavior agreement prior to being granted user accounts or access to information systems or data.

2. Promote collaboration on information security training efforts across the Department through the DHS Information Security Training Working Group (ISTWG) and share information on Component-developed training activities, methods, and tools, thereby reducing costs and avoiding duplication of effort. The Information Security Training Working Group is chaired by the DHS Enterprise Cybersecurity Awareness and Training Program Manager.

3. Ensure DHS Components abide by security training requirements listed in this directive, and that they prepare and submit information security awareness reports (including content, frequency, format, and distribution) for the DHS CISOD, as required.

(AU) Audit and Accountability Control Family

An audit is an independent review and examination of records and activities to assess the adequacy of the information system's controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in those controls, policies, or procedures. Accountability is the principle that an individual is entrusted to safeguard and control information/data, equipment, keying material, and is accountable to management for the use/misuse or compromise of that information system or resource.

The audit and accountability control family address the ability to maintain a record of system application and user activity. In conjunction with the appropriate tools and procedures, auditing can assist in detecting security violations, performance problems, and application flaws. This control family also serves as an insurance policy, ensuring that there are mechanisms in place to track and associate user, process, and system activity to events.

Whenever there is a deviation from the prescribed mode of operation, an examination of the audit and accountability controls can serve as a launch point to determine factors that may have caused this deviation or failure.

DHS's audit and accountability requirements, at a minimum, shall:

1. Develop, adopt, and adhere to a formal documented program for the monitoring, management, and review of system, application, network, and user activity. See OMB M-21-31.
2. Develop standards and procedures to guide the implementation and management of audit controls and records.
3. Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful,

unauthorized, or inappropriate information system activity.

4. Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
5. Provide audit record generation capability for relevant or auditable events identified by DHS. Per NIST definition, a relevant event is an occurrence (e.g., an auditable event or flag) considered to have potential security implications to the system or its environment that may require further action (noting, investigating, or reacting).
6. Audit records are sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records are reviewed as specified in the SP. The audit record contains at least the following information:
    - Identity of each user and device accessing or attempting to access the system
    - Time and date of the access and the logoff
    - Activities that might modify, bypass, or negate information security safeguards
    - Security-relevant actions associated with processing
    - All activities performed using an administrator's identity
7. When available, Components ensure implementation of enterprise auditing and recording of sessions (keystroke and graphical).
8. Review audit records monthly for financial systems or for systems hosting or processing PII. Unusual activity or unexplained access attempts are reported to the System Owner and to the Component CISO/ISSM. Ensure DHS systems' audit records and audit logs are protected from unauthorized access, modification, or destruction.
9. Record and retain audit logs in accordance with the DHS systems' Record Schedule or with the DHS systems' Record Schedule. At a minimum audit trail records are maintained online for at least 90 days. Preserve audit trail records for a period of three (3) years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease. DHS allocate appropriate audit record storage capacity in accordance with these requirements.
10. Ensure DHS evaluates the system risks associated with extracts of PII from databases. If the risk is determined to be sufficiently high, a procedure is developed for logging computer-readable data extracts. If logging these extracts is not possible, this determination is documented, and compensating controls identified in the SP.

(CA) Assessment, Authorization, and Monitoring Control Family

The assessment and authorization (A&A) process is implemented to ensure compliance with federal laws and regulations and is critical to minimizing the threat of breaches. Security and privacy assessments are conducted 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 and privacy requirements for the information system. Authorization is the process of accepting the residual risks associated with the initial and continued operation of DHS systems and granting approval to operate for a specified span of time. The Information Security Continuous Monitoring (ISCM) process is established to maintain an ongoing awareness of information security, vulnerabilities, and threats to support DHS risk management decisions. Control assessments evaluate the risk associated with the operation of a system and allow the Authorizing Official to ensure the system is operating at an acceptable risk prior to authorizing.

DHS's assessment, authorization, and monitoring requirements, at a minimum, shall:

1. Categorize information sensitivity in compliance with FIPS 199 as the basis to implement the appropriate DHS NIST 800-53 baseline controls. See Attachment CC for details.
    a) DHS Components assign the highest water mark for the impact levels (high, moderate, low) measured for the combined security objectives (confidentiality, integrity, and availability) for each DHS information system. DHS Components apply NIST SP 800-53, Revision 5, controls as tailored specifically to the security objective and impact level determined as described in NIST SP 800-53b, section 2.4.
    b) DHS Components implement the DHS Control Baseline, see Attachment CC for details on ODVs, and referencing FIPS Pub 200, *Minimum Security Requirements for Federal Information, and Information Systems*, based on the data's highest FIPS 199 impact level established for the combined security objectives (confidentiality, integrity, availability).
    i) DHS Components conduct their information systems security reviews in accordance with both FIPS 199 and NIST SP 800-53, Revision 5, for specification of security controls. NIST SP 800-53A are used for assessing the effectiveness of security controls and for quarterly and annual FISMA reporting.
        (1) All FISMA documentation must be consistent and up to date. ISCM waivers for FISMA reporting will be considered for the following types of systems:
            (a) Software Only (internally hosted cloud environment)
            (b) Software as a Service (SaaS)
            (c) FedRAMP P-ATO systems

(d) "Stand Alone" systems

2. Ensure that only authorized systems including, but not limited to, workstations, servers, cloud computing applications, software applications, mobile devices, networks, and data repositories have an authorization to operate (ATO) in accordance with DHS's business needs. See the DHS Security Authorization Guide (SAG) for additional details.
3. Components are required to leverage automated tools (e.g., CSAM) for system authorization for analysis but must also provide manual expert analysis through the package review process. Automated tools will also provide initial data categorization and security responses, focusing on tagging and managing access to sensitive documents.
4. Artifacts in support of *new* ATOs are not older than 12 months. Existing artifacts are not valid beyond the life of any current ATO unless the system is enrolled in ongoing authorization program, requiring continuous assessment to produce the annual assessment SAR and ATO renewal. See the DHS Ongoing Authorization Guide for additional details.

    a) DHS Components assign a common controls package for systems providing common control infrastructure (e.g., hosting providers such as cloud IaaS). DHS Components assign a common control provider to share controls between systems (e.g., at hosting centers). The authorization package of those common controls is shared with those operating under the controls in accordance with the individual service level agreements and with those leveraging those services.

    i) DHS Common Control Policy

    ii) FedRAMP Control Baselines

a) For systems not entering Ongoing Authorization (OA) Program, Components authorize DHS systems at Initial Operating Capability (IOC) and every three (3) years thereafter, or sooner, whenever a major change occurs.

b) For Systems entering the Ongoing Authorization (OA) Program, OA Components authorize DHS systems at Initial Operating Capability (IOC), through submission of an OA Admission Letter and renewed thereafter annually as a part of the annual assessment approval, with 100% of controls tested within an 3 year period, in accordance with OMB A-130, NIST guidance and DHS Ongoing Authorization Methodology. (See DHS Security Authorization Templates.)

c) DHS enterprise services are required to provide a catalog of common controls that have been assessed and authorized by the AO of that service.

d) Components leveraging FedRAMP Provisional Authority to Operate (P-ATO) Authorizations, Agency Authorized Systems, or sponsor an agency authorization for a cloud system, are responsible for reviewing, monitoring and, or

maintaining all common activities for that CSP. This includes:

i) In the initial DHS ATO process, Components must assess the risk of the system and review CSPs documents (e.g., System Security Plan (SSP), Security Assessment Report (SAR)) as a part of their security package in order to validate the control implementations meet DHS requirements. DHS must decide if the risk is acceptable, and if the system meets DHS requirements. DHS must review and determine if FedRAMP P-ATO Cloud Service Provider's baseline controls, that are not customer responsible controls, meet, or exceed, DHS requirements and whether they are inheritable by the component.

ii) Responsibilities for DHS agency ATOs include monitoring all Cloud Service conmon activities (both provider and agency instance) according to the DHS Security Authorization Guide based on FedRAMP requirements (e.g., monthly vulnerability scans, POA&M and vulnerability management, significant change requests, corrective action plans, etc.,).

(1) FedRAMP Agency Authorizations and DHS ATOs: DHS is responsible for coordinating conmon with the cloud service provider for review

(2) FedRAMP Joint Authorization Board *Provisiona*l *Authority to Operate* (P-ATO): DHs is responsible for reviewing the monthly conmon one pager available in the public customer facing folder.

iii) All DHS cloud service ATOs must follow and adhere to FedRAMP requirements. See FedRAMP Authorization Roles and Responsibilities for additional details.

2) Assess security and privacy controls periodically (e.g., Annual Assessment) in DHS information systems to determine if the controls are implemented according to current NIST SP 800-53, Revision 5, requirements.

3) Develop and implement POA&Ms designed to correct deficiencies and reduce or eliminate vulnerabilities in DHS information systems.

a) Develop plans for vulnerability remediation management and POA&Ms that adhere to federal timeline requirements outlined below, unless otherwise noted.

b) Item identified during an assessment (source of weakness) must be selected for all POA&Ms. This may include, but is not limited to, annual assessments, security assessment findings that produce a Security Assessment Report (SAR), audit findings [OIG, Government Accountability Office (GAO)], OMB Circular A-123 Reviews, IT Acquisition Reviews (ITARs), Enterprise Architecture Center of Excellence (EA COE), management decisions, and Information Security Vulnerability Management (ISVMs).

c) If not remediated within 30 days of detection, POA&Ms must be

created for all unremediated technical findings, as cited in the most current 4300A Attachment H *Plans of Actions and Milestones (POA&M) Guide*, hereafter known as Attachment H, POA&M Guide, and tracked on the Weakness Remediation Scorecard, including ISVMs, and the required timeline for remediating technical findings, such as Software vulnerabilities and misconfigurations outlined, unless otherwise noted, are as follows:

i) Critical vulnerabilities associated with DHS systems must be remediated within 15 days of initial detection. [Binding Operational Directive (BOD) 19-02 (April 29, 2019)]

ii) High vulnerabilities associated with DHS systems must be remediated within 30 calendar days of detection.

iii) Moderate vulnerabilities associated with DHS systems must be remediated within 90 calendar days of detection.

iv) Low vulnerabilities associated with DHS systems must be remediated within 180 calendar days of detection.

4) POA&M technical remediations are coordinated between the system ISSO, System Administrator/Engineer responsible for the maintenance and configuration of the system, and the System Owner.

a) ISSOs track and coordinate the completion of milestones carried out by the System Administrator/Engineer responsible for the system maintenance and configuration of the system impacted by the finding.

b) The responsible System Admin/engineer must provide the root cause for each POA&M, see DHS 4300Aattachment H *Plan of Action and Milestones (POA&M) Guide* for instructions and for A-123 related findings see the Root Cause template here, ISSMs track and validate the evidence of POA&Ms closures which impact all the systems under their purview.

c) Control Validation (meaning the testing of any impacted controls) after POA&M remediation have been completed, and the evidence of testing is provided for POA&M closure. See NIST SP 800-53A for details on required testing and evidence methods and guidelines.

d) POA&M closures require validation of remediation evidence submitted (e.g., remediation scans, configuration validation, hardware replacement, process validation, attestation, etc.) prior to closure.

e) The Information System Security Manager (ISSM) of the system is responsible for verifying this evidence and completing the final closure of the POA&M.

i) To close out remediation activities for FY findings related to Information Technology Notice of Finding and Recommendation (ITNFR), OMB A-123 assessments, CISOD requires Components to upload and

provide artifacts (e.g., OMB A-123, ITNFR V&V packages, etc.,) as evidence that the control was remediated.

f) All POA&Ms are required to be created from the Information Assurance Compliance System (IACS), (e.g., CSAM) if unremediated 30 days after detection.

g) Repeat findings from assessments must be tracked as part of the existing open POA&Ms if one exists. The original POA&M may not be closed or cancelled. A new POA&M should only be created for any additional unique findings that were not part of a previously created open POA&M.

5) Ensure that this Policy Directive applies to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS information unless they meet ATO control requirements or an approved waiver or risk acceptance memo, has been granted. This includes prototypes, pilots, telecommunications systems, external third-party services, or cloud services, and all other systems in all phases of the Systems Engineering Life Cycle (SELC).

6) When a DHS Component is unable to fully comply with any portion of this Directive, it may request a waiver, with the exception of any vulnerability, or finding, that impacts certain requirements provided by CISOD such as the DHS Critical Controls list, Executive Directives, Binding Operational Directives, or Emergency Orders. Waiver requests are routed through the DHS Component's ISSO for the system, to the Component's ISSM, and then to the Component's CISO for final approval. All submitters coordinate with the Component Authorizing Official prior to submission to the Component CISO.

7) If a finding is reported in an audit report, and the weakness is not successfully remediated within 12 months, the DHS Component ISSO/ISSM must submit a Risk Acceptance Request form, 4300A Attachment B *Waiver and Risk Acceptance Request Form* submitted by the Component CISO in coordination with the Authorizing Official (AO) for approval.

a) If the finding exists in a system processing PII, see Privacy Office Security Policy for waiver and risk acceptance requirements.

b) For CFO Designated Systems Waiver and risk acceptance requests must follow all requirements for the Component's Chief Financial Officer (CFO) requirements

c) For Privacy Sensitive Systems Waiver and risk acceptance requests for privacy sensitive systems must follow all waiver and risk acceptance guidance from the Component Privacy office and Senior Privacy Point of Contact (PPOC) .

d) Tier 1 High Value Assets: Components must also provide a signed memo from the component's CISO validating and approving the corrective actions to remediate the deficiency. Both the Components' signed memo and remediation plan will be reviewed and signed by the DHS' Senior Accountable Official for Risk Management or SAORM. Components must provide updates every 30 days until all findings have been remediated. For additional requirements, please see 4300A Attachment H, *POA&M Guide*, for details. Waiver and risk acceptance requests for

these systems and programs must follow the requirements listed above and must be routed to the DHS CISO for approval.

8) An approved waiver does not bring the system into compliance with policy; it is an acknowledgement by the component CISO of the system's non-compliance with policy and that an acceptable plan to remediate the weakness has been provided, and scheduled within 12 months of detection, and compensating controls have been documented as a part of the remediation plan and have been implemented according to the approved milestones.

a) In all cases, waivers are requested for a period no longer than 12 months based on the required remediation strategy with countermeasures and justification provided as a part of the submission. Otherwise, the Component CISO must submit a Risk Acceptance form (4300A Attachment B) in coordination with the Component CISO for final approval by the Component Authorizing Official (AO).

b) POA&M waivers should be requested only when remediation of controls findings require additional resources or time to implement. Waivers should include justifications and countermeasures for required controls being waivered and not implemented according to federal requirements.

c) See Attachment B for additional instructions on waiver requirements and submitting waiver requests and risk acceptance memos.

9) Component CIOs and/or CISOs are allowed to approve risk acceptances for the following topics without DHS CISO approval:

a) NIST SP 800-53 controls that do not have a related requirement in 4300A policy

b) Systems on a closed network with no connection to the internet or external systems

c) Continued use of end of life (EOL) systems while modernization efforts are underway

d) Session lock, session termination, and screensaver requirements for:

(i) Kiosks

(ii) Workstations located in 24/7 secure locations, supporting continuously monitored mission traffic

Component-approved risk acceptances must be submitted to the DHS CISO for documentation and informational purposes.

10) Authorize the operation of DHS information systems and any associated information system connections. The DHS *Security Authorization Guide (SAG)* describes detailed processes governing security authorizations. Detailed information for creating and managing POA&Ms is published in the DHS Policy Directive 4300A, *Information Technology System Security Program (ITSSP), Sensitive Systems*, Attachment H: "Plan of Action and Milestones (POA&M) Process Guide."

a) DHS Components are accepted into the DHS Ongoing Authorization (OA) Program only with concurrence from the Component's CIO with coordination with the Component CISO and Authorizing Official. All submissions are considered by the DHS CISOD using objective eligibility requirements as outlined in the DHS OA Methodology.

b) Eligible DHS Components may submit requests for systems to join the DHS OA Program. Systems submitted require a valid ATO at least 60 days from expiration at date of submission (further details are found in the latest version of the DHS Ongoing Authorization Methodology.

c) Monitor security (e.g., all required Continuous Monitoring Activities and Annual Assessments) and privacy controls on an ongoing basis to ensure the continued effectiveness of the controls for the OA requirements.

d) The DHS Enterprise Security Operations Center (NOSC) exchanges information with DHS Component Security Operations Centers (SOCs), Network Operations Centers (NOCs), the Homeland Secure Data Network (HSDN) SOC, the Intelligence Community, and with external organizations in order to facilitate the security and operation of the DHS network. This exchange enhances situational awareness and provides a common operating picture to network managers. The operating picture is developed from information obtained from "raw" fault, configuration management (CM), accounting, performance, and security data. This data is monitored, collected, analyzed, processed, and reported by the NOCs and SOCs.

e) The DHS NOSC is responsible for communicating other information such as incident reports, notifications, vulnerability alerts and operational statuses to DHS Component SOCs, Component CISOs/ISSMs, and other identified Component points of contact.

f) The DHS NOSC portal implements role-based user profiles that allow DHS Components to use the website's incident database capabilities. Users assigned to DHS Component groups are able to:

i) Enter incident information into the DHS NOSC incident database
ii) Generate preformatted incident reports
iii) Initiate queries of the incident database
iv) View current FISMA incident reporting numbers
v) Automate portions of the ISVM program
vi) Automate approved service providers. The controlled interfaces are authorized at the highest portions of the vulnerability assessment program

11) Interconnections between DHS and non-DHS systems must be established only through the Trusted Internet Connection (TIC) and by security level of information (see NIST FIPS 199 for information security impact categorization details) on the network. Connections with other Federal agencies are documented based on interagency agreements,

Memorandums of Understanding (MOU), Memorandum of Agreement (MOA), Service Level Agreements (SLA), or ISA. For additional details about DHS MOU/MOA requirements see link here.

12) Ensure DHS Components document all interconnections to the DHS OneNet with an ISA signed by the OneNet AO and by each appropriate AO.

13) Ensure that ISAs are reissued every three years or whenever any significant changes have been made to any of the interconnected systems.

14) Ensure that ISAs are reviewed and updated at a minimum every three years or as needed as a part of the annual FISMA self-assessment requirement.

15) Ensure DHS Components document interconnections between their own and external (non- DHS) networks with an ISA for each connection.

16) Ensure the Department and DHS Components implement Trust Zones by means of Policy Enforcement Points (PEP), as defined in the DHS Security Architecture Framework.

17) Interconnections between two authorized DHS systems do not require an ISA if the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements are accounted for in the SPs or are described in another formal document, such as an SLA or contract, and the risks have been assessed and accepted by all involved AOs. See DHS Security Authorization Guide (SAG).

(CM) Configuration Management Control Family

Configuration management is the act of managing the configuration of all hardware and software elements of information systems and networks and assessing the security implications when changes occur. The initial configuration baseline should require approval through a change request, requiring security impact analysis, prior to the system being developed. Also, it would be helpful to specify CM requirements apply to all configuration items and are not limited to "production" systems.

The configuration of a DHS system and its components has a direct impact on the security posture of that system. Changes to the configuration of DHS systems are often needed to align with changing business functions and services, and information security needs. However, changes can adversely impact the previously established security posture; therefore, effective configuration management is vital to the establishment and maintenance of security of information and systems. The DHS security-focused configuration management process is critical to maintaining a secure state under normal operations, contingency recovery operations, and reconstitution to normal operations.

To effectively execute its configuration management policies and requirements , DHS, at a minimum, shall:

1. Establish and maintain baseline configurations and inventories of DHS information systems.
   a. The CIO, in cooperation with each of the DHS Components' senior officials, ensures that every DHS computing resource is identified as an information system or as a part of an information system, either as a Major Application (MA) or General Support System (GSS).
   b. Security-relevant management processes and tools comply with applicable NIST-standard protocols and conventions as described in NIST SP 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP)*, including the Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE), and Common Vulnerabilities and Exposures (CVE).
   c. Document, implement, and maintain configuration and change management processes.
   d. DHS Components develop and maintain a Configuration Management Plan (CMP) for each information system as part of its SP. All DHS systems are under the oversight of the Change Management Board (CCB)

2. Establish and enforce security configuration settings for DHS IT products employed in DHS information systems.
   a. DHS Components ensure that DHS information systems follow the hardening guides for operating systems and the configuration guides for applications published by the DHS CISOD. See Attachment CC *DHS Control Baselines and ODVs* based on NIST SP 800-53, Revision 5.
3. Monitor and control changes to the baseline configurations and to the constituent components of DHS information systems (including the installation of patches, hardware, software, firmware, and documentation) throughout the system's development life cycles.
   a. Information security patches are installed in accordance with component CM plans, following the timeline for remediation of software vulnerabilities and misconfigurations, under section 4.c. of the Assessment, Authorization and Monitoring (CA) control family and 4300A Attachment H, the POA&M management Guide, and within the timeframe or direction stated in the ISVM message published by the DHS ESOC.
4. Develop and implement effective plans and be adequately staffed to ensure the ability to reverse or undo any deployment or implementation that has negatively impacted the working environment.
5. Ensure that information systems and networks are appropriately documented in such a way as to allow others to fully understand the system operation picture and configuration.

(CP) Contingency Planning Control Family

Contingency planning refers to interim measures to recover information systems after a

disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods. The main goal of contingency planning is the restoration to normal modes of operation while mitigating against loss of data with minimum cost and disruption to normal business activities after an unanticipated event.

DHS must develop contingency planning processes to prepare for, detect, react to, and recover from events that threaten the security of DHS information system resources and assets. The appropriate level of IT business continuity management must be in place to sustain the operation of DHS's critical IT services to support the continuity of vital business functions and the timely delivery of critical automated business services. Appropriate planning and testing processes must be in place to ensure that, in the event of a significant business interruption, critical production environments can be recovered and sustained to meet DHS's business requirements. This policy covers mainframe, distributed environments, and cloud- hosted environments.

DHS's contingency planning requirements, at a minimum, shall:

1. Ensure the DHS CIO provides guidance, direction, and authority for a standard DHS-wide process for contingency planning of information systems.
2. DHS Components shall identify DHS's essential mission and business functions and associated contingency requirements.
3. System Owners are responsible for developing and documenting information system Contingency Plans (CPs) for their information systems, managing plan changes, and distributing copies of the plan to key contingency personnel.
4. Component CIOs review and approve DHS Component-level information system CPs.
5. Establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for DHS information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
6. Implement backup policy and procedures for every DHS Component information system.
7. Ensure continuity planning is in alignment with the DHS Information Security Program due to the complementary and mutually reinforcing efforts. For essential functions, the Federal Continuity Directives, the DHS Continuity Program Directive, and DHS Continuity Plan require Business Process Analysis (BPA) and Business Impact Analysis (BIA), which enables the identification of critical DHS assets and systems. Once critical systems are identified, continuity planning shall address two different but complementary elements: Continuity of Operations Planning (COOP) and CP. See NIST 800-34 for details.
8. Maintain Vital Records:
    a. Vital records are electronic and hardcopy documents, references, databases, and information systems needed to support essential functions under the full spectrum of

emergencies.

i. Categories of vital records may include:

1. Emergency operating records: emergency plans and directive(s); orders of succession; delegations of authority; staffing assignments; selected program records needed to continue the most critical agency operations; and related policy or procedural records.
2. Legal and financial rights records: records that protect the legal and financial rights of the Government and of the individuals directly affected by its activities. For example, accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as "rights-and-interests" records.
3. Records used to perform national security preparedness functions and activities in accordance with Eos.

9. When available, a DHS-wide process for COOP is used in order to ensure continuity of operations under all circumstances.
    a. A DHS system has contingency capabilities commensurate with the availability security objective. The minimum contingency capabilities for each impact level are as follows:
        i. High impact – System functions and information have a high priority for recovery after a short period of loss.
        ii. Moderate impact – System functions and information have a moderate priority for recovery after a moderate period of loss.
        iii. Low impact – System functions and information have a low priority for recovery after prolonged loss.
    b. DHS Components develop, test, implement, and maintain continuity of operations plan(s) and programs, in compliance with the DHS Continuity Plan and Program, to ensure the recovery and continuation of DHS essential functions. See FISMA 2014.
10. Test the CP for all DHS systems to determine the effectiveness of the CP and to identify potential weaknesses in the plans.
    a. Components coordinate CP testing and/or exercises as appropriate, using COOP-related plans for systems with moderate and high availability FIPS 199 categorizations.
11. Provide contingency planning training to all system users.
12. Establish an alternate storage site to permit the storage and retrieval of DHS system backup information.

(IA) Identification and Authentication Control Family

Authentication is the process of establishing confidence in user identities electronically presented to an information system. Individual authentication is the process of establishing an

understood level of confidence that an identifier refers to a specific individual. Authentication focuses on confirming an individual's identity, based on the reliability of the individual's credentials. Authentication of user identities is accomplished using passwords, tokens, public key infrastructure (PKI) certificates, key cards, biometrics, or in the case of multi-factor authentication, some combination therein. The identification and authentication controls provide DHS security policy requirements for the management of user identification and authentication, which is required to safeguard access to information systems and critical business processes/resources. DHS users include employees or individuals that DHS considers having the equivalent status of employees, including contractors and third-party entities or business partners.

Digital Identities (e-authentication) is needed to ensure that online Government services are secure, and that individual privacy is protected. Each DHS system is evaluated to determine whether e-authentication requirements apply. Only federated identity providers approved through the Federal CIO Council's Identity, Credentialing, and Access Management's (ICAM) Trust Framework Provider Adoption Process (TFPAP) is used. Components should see www.IDmanagement.gov for details regarding the Federal Identity, Credentialing, and Access Management (FICAM) initiative.

E-authentication guidance is provided in the following:

- OMB M-04-04, *E-Authentication Guidance for Federal Agencies*
- NIST SP 800-63, *Electronic Authentication Guideline*

DHS's identification and authentication requirements, at a minimum, shall:

1) Identify information system users, processes acting on behalf of users, or devices, and authenticate the identities of those users, processes, or devices, as a prerequisite to allowing access to DHS information systems.
   a) Digital and Other Electronic Signatures
      i) Pursuant to Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), OMB Memorandum M-00-10, Procedures and Guidance on Implementing of the Government Paperwork Elimination Act requires executive agencies to provide the option for electronic maintenance, submission, and disclosure of information when practicable as a substitute for paper, and to use and accept electronic signatures. Minimally, all electronic correspondence and official digital documents need a digital signature except where a wet signature is required.
      ii) Electronic signatures, including digital signatures, are implemented by applications with the necessary security controls and practices such that:
         (1) The signer cannot successfully repudiate that he/she intended to sign, or that

he/she applied the electronic signature; and

(2) The integrity of the signed content cannot be successfully challenged.

iii) The following requirements are met when implementing legally binding signatures using digital signature or another electronic signature method:

(1) The signer uses an acceptable electronic form of signature.

(2) The electronic form of signature is executed or adopted by a person with the intent to sign the electronic record.

(3) The electronic form of signature is attached to or associated with the electronic record being signed.

(4) There is a means to identify and authenticate a particular person as the signer; and

(5) There is a means to preserve the integrity of the signed record.

iv) Please refer to the DHS Electronic Signature Policy Guidance, 4300A Attachment Z, and NIST SP 800-63 for additional guidance on electronic signature requirements.

2) Uniquely identify and authenticate DHS devices before establishing a remote or network connection implementing technical requirements according to NIST SP 800-63, and at a minimum includes:

a) Existing physical and logical access control systems are upgraded to use PIV credentials, in accordance with NIST and DHS guidelines. See NIST P 800-63 and HSPD 12 for additional details.

b) DHS Components determine the appropriate assurance level for e-authentication by following the steps described in OMB M-04-04, E-Authentication Guidance for Federal Agencies.

c) If fingerprint sensors are authorized for use, then the sensors must be touch based (vs. swipe-based) and read and process data in a trusted execution environment separated from access by other processes.

d) When approved laptops or devices are in use (e.g., at residence (telework), on site at a government facility, or when traveling with travel approved laptops and devices), passwords, tokens and smart cards are not stored on or with the laptop or other mobile computing devices.

e) Wireless mobile devices that store, process, or transmit sensitive information implement full-disk encryption using current NIST FIPS 140 validated encryption modules and strong complex passwords prior to receiving sensitive information. A strong complex password is required to decrypt after any power cycling or restart. For additional requirement details see NIST SP 800-124, "*Guidelines for Managing the Security of Mobile Devices in the Enterprise.*"

f) OMB M-22-09 Identity Task requires the removal of regular password rotation and use of special characters "Agencies must remove password policies that require special characters and regular password rotation from all systems within one year."

g) Manage system identifiers by receiving authorization from DHS to assign an individual, group, role, or device identifier.
h) Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Eos, directives, policies, regulations, standards, and guidelines for such authentication. See NIST SP 800-63 for encryption, digital certificate, and multi-factor authentication requirements.
i) Uniquely identify and authenticate non-DHS users or processes acting on behalf of non-DHS users. Follow NIST SP 800-63 to determine password security and complexity for DHS systems where user identity is authenticated by password. As DHS moves to a Zero Trust Architecture, passwords policies will remain in effect until passwords are no longer authorized for use on DHS systems." For non-DHS systems, password use will be regulated by the owner of the system.
j) Privileged network users use the DHS HSPD-12 credential for authentication to all DHS Privileged network user accounts.

(IR) Incident Response Control Family

An incident is a violation or imminent threat of violation of information security policies, acceptable use policies, or standard computer security practices. Incidents may result from intentional or unintentional actions. Incident response relates to action taken in reaction to an incident occurrence. These incidents can severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data. To help combat the disruptive short- and long-term effects of security incidents, DHS is required to implement and maintain a security incident reporting and handling capability.

Quickly responding to incidents provides a mechanism for controlling the impact of the incident on DHS information systems; therefore, all DHS users must understand their incident response responsibilities and the actions they should take if an incident is suspected or has occurred. To accomplish this, users require training in incident detection and response.

DHS's incident response requirements at a minimum, shall:

1) Establish an operational incident handling capability for DHS information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
2) Track, document, and report incidents to appropriate DHS officials and authorities.
   a) The DHS NOSC is the central coordinating and reporting authority for all Sensitive and National Security computer security incidents throughout the Department.
3) Conduct tests and exercises in a controlled environment to determine the effectiveness of DHS's incident response capability and to improve on that capability.

4) Report PII data breach(s) to the Cybersecurity and Infrastructure Security Agency (CISA) promptly.
   a) PII or Sensitive Data Spillage see:
      i) DHS Components follow the DHS Privacy Incident Handling Guidance.
5) Ensure DHS Components establish and maintain a continuous 24x7 incident response capability.
6) Ensure DHS personnel follow DHS CISOD procedures for detecting, reporting, and responding to information security incidents in accordance with the DHS NOSC Concept of Operations (CONOPS). Reports are classified at the highest classification level of the information contained in the document. Un-sanitized reports should be marked and handled appropriately.
   a) DHS follows Cybersecurity Services Provider (CSP) Evaluator Scoring Metrics (ESM) requirements
      i) Components must meet minimum maturity for IR related metrics. See DHS Cybersecurity Services Program Authorization for details.
7) Respond to cyber-attacks, events, and incidents pertaining to DHS assets through the DHS NOSC. When an external organization is involved, the DHS NOSC coordinates with the external organization through United States Computer Emergency Readiness Team (US-CERT), except in time- sensitive cases where a response requires direct contact with the external organization.
8) Enable the DHS NOSC to report incidents to US-CERT in accordance with the DHS NOSC CONOPS. Also, all reporting timelines and report requirements must be reflected in the component to the Incident Response Plan (IRP).
9) Receive classified spillage incident reports, in accordance with the IRP, and support the DHS CSO containment and cleanup efforts. All spillage incidents must also be reported to CSO.
10) Ensure DHS Component SOCs report incidents to the DHS NOSC, which provides them operational oversight and guidance. SOC oversees the handling of all incidents occurring and coordinates the sharing of incident information with DHS NOSC.
    a) Components may outsource to any approved CSP within the Department
11) Implement the Department logging strategy through the DHS NOSC, coordinated with Component SOCs, to enable endpoint visibility and Departmental situational awareness. The DHS NOSC is responsible for monitoring shared infrastructure such as the Trusted Internet Connection (TIC), Policy Enforcement Points (PEP), and Email Secure Gateway (EMSG). Component SOCs are responsible for monitoring at a minimum internal enclave network traffic and internal host network and host-based activity.
12) Maintain a cyber threat intelligence fusion center that performs cyber threat intelligence activities relevant to all of DHS through the DHS NOSC. The fusion center must have the ability to process and integrate classified Cyber Threat Intelligence (CTI) information up to

the TS/Secure Compartmented Information (SCI) level.

13) Provides ISVM messages and vulnerability assessment capabilities through the DHS NOSC and DHS Components must comply with the ISVMs. DHS Component SOCs develop a robust vulnerability management capability to compliment the DHS NOSC.
14) Ensure DHS Component SOCs report operationally to their respective Component CISO. Each CISO exercises oversight over their Components' information security operations functions, including the Component SOCs.
15) Provide 24/7 leadership (i.e., a federal employee) and direction at all NOSC locations.
16) Ensure DHS Components maintain a full SOC capability or outsource SOC capability to the DHS NOSC. The DHS NOSC provides SOC services to DHS Components in accordance with formal agreements.
17) Ensure DHS Components develop and publish a Configuration Management (CM) Plan consisting of internal computer security incident response plans and incident handling procedures.
18) Ensure DHS Component SOCs report incidents to the DHS NOSC only. Reports should not be shared with any external agency or organization.
19) Publish incident response testing and exercise scenarios, as required. All tests should be approved by the CISO and NOSC prior to being conducted. See NIST SP 800-62, 800-84 for testing requirements.
20) Ensure DHS Components coordinate all external Law Enforcement (LE) involvements through the DHS NOSC. All DHS Components should follow-up with the DHS NOSC for LE updates. Exceptions are only made during emergencies where there is a risk to life, limb, or property. In cases of emergency notification, DHS Components notify the DHS NOSC as soon as possible, by the most expedient means available.
21) Security incidents may include LE or counterintelligence (CI) elements, such as maintaining a chain of custody. All incidents containing a LE/CI aspect are coordinated with the DHS CSOD through the DHS NOSC.

(MA) Maintenance Control Family

Regular maintenance of information systems mitigates some of the threats to the system. The maintenance control family address policies to ensure that the systems and services used by DHS are maintained and repaired properly. Maintenance requirements apply to all types of maintenance to any system component (hardware, firmware, operating system, and applications). System maintenance also includes components not directly associated with information processing or retention, such as scanners, copiers, and printers. This Policy Directive reflects the predominant business model under which maintenance functions are generally outsourced to IT service providers. The federal function, assigned to the CIO, is one of oversight to ensure service providers maintain IT assets consistent with federal standards. As a

result, responsibilities are assigned to designated agents of the Federal CIO which can include DHS Program Offices, contractors, or other federal agencies.

DHS's system maintenance requirements at a minimum, shall:

1) Perform periodic and timely maintenance on DHS information systems.
2) Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
3) Schedule, document, and review records of maintenance, repair, or replacement on system components in accordance with manufacturer or vendor specifications and/or DHS requirements.
4) Employ effective maintenance tools, such as hardware/software diagnostic test equipment and hardware and software packet sniffers.
5) Establish a process for maintenance of personnel authorization and supervise the maintenance activities of personnel who do not possess the required access authorizations.
6) Obtain maintenance support and spare parts for critical systems, to support DHS-defined recovery time objectives.

(MP) Media Protection Control Family

Information resides in many forms and can be stored in different ways. Media controls are protective measures specifically designed to safeguard electronic data, the physical media they are stored on (tape, disk, flash-memory, etc.) and hardcopy information (paper, microfilm, etc.). This policy addresses the protection, marking, sanitization, production input/output, and disposal of media containing sensitive information. All levels of DHS management must ensure that employees, contractors, vendors, and other third-party entities protect information system media, both paper and digital; limit access to information stored on information system media to authorized users; and sanitize or destroy information system media before disposal or release for reuse. See NIST SP 800-88, *Guidelines for Media Sanitization*, February 2015, and NIST SP 800-209, *Security Guidelines for Storage Infrastructure*, October 2020, for additional details

DHS's media protection requirements, at a minimum, shall:

1) Limit access to information system media to authorized users.
   a) DHS Components control the transport of information system media containing sensitive information, outside of controlled areas and restrict the pickup, receipt, transfer, and delivery to authorized personnel.
2) Protect information system media and sanitize or destroy information system media

before disposal or release for reuse.

a) DHS Components ensure that any information systems storage medium containing sensitive information is sanitized using approved sanitization methods before it is disposed of, reused, recycled, or returned to the owner or manufacturer. For additional requirements details, please see NIST SP 800-88.

3) Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.
   a) Media determined by the information owner to contain sensitive information must be appropriately marked in accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information.
4) DHS Media storage requirements, shall include at a minimum the following:
   a) DHS Components ensure that all media containing sensitive information, including hard copy media, backup media, and removable media such as Universal Serial Bus (USB) drives, are stored when not in use in a secure location (e.g., a locked office, room, desk, bookcase, file cabinet, locked tape device, or in other storage that prohibits access by unauthorized persons).
   b) DHS Components follow the procedures established in DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information for the transportation or mailing of sensitive media.
   c) Ensure that System Owners develop and enforce procedures to ensure proper malware scanning of media prior to installation of primary hard drives, software with associated files, and other purchased products.

(PT) Personally Identifiable Information Processing and Transparency Control Family

The purpose of the Privacy Act of 1974 is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them. Individuals are active participants in the decision-making process regarding the collection and use of their PII. The controls in this family enhance DHS's ability to comply with the Privacy Act and the public confidence in DHS decisions made based on PII. Each DHS user has a right to decide when and whether to share personal information, how much information to share, and the circumstances under which that information can be shared.

DHS's privacy program is a foundation of information security. Privacy is more than security and includes the principles of transparency, notice, and choice. The privacy authorization controls focus on ensuring that DHS managers and systems have proper authority and authorization to

collect, store, and make use of privacy-related information.

DHS's privacy requirements, at a minimum, shall:

1) Determine and document the legal authority that permits the collection, use, maintenance, and sharing of PII in support of a specific DHS program or system need.
2) Identify and document the purpose for which PII is collected, used, maintained, and shared in its privacy notices.
3) Develop and disseminate guidelines for the sharing of PII externally.
4) Require users to consent to the processing of their PII prior to its collection.
5) Provide mechanisms for users to redress the use of their PII residing in DHS systems.
6) Make privacy notices available to users to help them understand how their information is being processed.
7) Make available Privacy Act Statements to DHS users, including notice of the authority of DHS offices or systems to collect their PII.
8) Provide users the ability to access their PII information maintained in DHS systems of records.
9) To promote privacy compliance within the Department, the Office has published official Department guidance regarding the requirements and content for Privacy Threshold Analysis (PTAs), Privacy Impact Assessment (PIAs), and System of Records Notice (SORNs). Privacy Compliance Guidance can be found on the DHS Privacy Office website and in the DHS Policy Directive 4300A, "*Information Technology System Security Program , Sensitive Systems*," Attachment S, "Compliance Framework for Privacy Systems."
10) OMB CircularA-130 requires a PTA that provides a high-level description of an information system including the information it contains and how it is used. The PTA is used to determine and document whether a PIA and/or SORN are required
    a) The PTA provides a high-level description of the system, including the information it contains and how it is used. PTAs are required whenever a new information system is being developed or an existing system is significantly modified, not to exceed three (3) from the original initiation date. DHS 4300A Attachment S defines the PTA requirements.
    b) System Owners and Program Managers are responsible for writing the PTA as part of the SELC process.
    c) The Component Privacy Officer or Privacy Points of Contact (PPOC) reviews the PTA and forwards it to the DHS Privacy Office, who determines whether a PIA and/or SORN are required.
11) A PIA is a publicly released assessment of the privacy impact of an information system and

includes an analysis of the PII that is collected, stored, and shared.

a) PIAs are required (as determined by the PTA) whenever a new information system is being developed or an existing system is significantly modified. PIAs are the responsibility of the System Owner and the Program Manager as part of the SELC process. OMB Memorandum M-03-22, DHS MD 0470.1, and the DHS Policy Directive 2017-01, *Privacy Policy Memorandum*.

b) PIAs are one tool that DHS uses to convey public notice of information practices and the privacy impact of Department programs and activities.

c) The Department also uses web privacy policies, SORNs, and Privacy Act Statements to provide effective public notice of program privacy practices.

d) PIAs also document how DHS makes individuals active participants in the decision-making process regarding the collection and use of their PII.

12) A SORN describes the categories of records within a system of records and describes the routine uses of the data and how individuals can gain access to records and correct errors.

a) The Privacy Act of 1974 requires a SORN when PII is maintained by a Federal agency in a system of records and the PII is retrieved by a personal identifier. A system of record is "*a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.*"

b) The SORN describes the categories of records and individuals in the system of record; the routine uses of the data; how individuals can gain access to records pertaining to them and correct errors. The term "system of records" is not synonymous with "information system" and can include paper as well as electronic records.

c) SORNs maybe written to cover the records in a single group of records or a single information system or they may be written to cover multiple groups of records or multiple information systems.

d) Information systems that are considered a system of record are not designated operational until a SORN has been published in the *Federal Register* for thirty days. OMB has issued the benchmark references for development of SORNs: *Privacy Act Implementation, Guidelines and Responsibilities* (July 9, 1975); and Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals to OMB Circular A-130.

13) DHS has published MD 047-01-001, Privacy Policy and Compliance, (October 6, 2005); and *Official DHS Guidance on System of Records and System of Records Notices.* Information systems that are considered a system of record keep an accurate accounting of disclosures of information shared outside of the system.

a) A SORN is required when PII is maintained by a federal agency in a system of records where information about an individual is retrieved by a unique personal identifier. SORNs are published in the Federal Register.

b) Information systems containing PII are not designated operational until a SORN has been published in the Federal Register for 30 days.

c) Programs provide individuals the ability to have access to their PII maintained in its system(s) of records.

d) DHS publishes rules and regulations governing how individuals may request access to records maintained in a system of records.

e) Programs publish access procedures in SORNs.

f) DHS adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

g) In their privacy notices, including SORNs, DHS Components describe the purpose(s) for which PII is collected, used, maintained, and shared.

h) DHS Components include Privacy Act Statements on all 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.

i) DHS Components establish 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.

j) DHS provides a process for individuals to have inaccurate PII maintained by the Department corrected or amended, as appropriate.

k) OMB requires each SORN to be reviewed every two (2) years to ensure that it accurately describes the system of records. This process is called the Biennial SORN Review Process.

14) DHS Privacy Office works with Components to ensure that SORN reviews are conducted every two years following publication in the Federal Register..

i) DHS Components review and republish SORNs every two (2) years.

15) OMB M-06-16, *Protection of Sensitive Agency Information* requires that agencies protect PII that is physically removed from Department locations or is accessed remotely. Physical removal includes both removable media and media in mobile devices (e.g., laptop hard drives).

1) Programs may use PII either as specified in public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Sharing PII outside the Department is restricted to a purpose compatible with the purpose for which the PII was collected.

a) PII and Sensitive PII (SPII) removed from a DHS facility on removable media, equipment or mobile devices are encrypted unless the information is being sent to an individual as part of a Privacy Act or Freedom of Information Act (FOIA) request.

b) If PII and SPII can be physically removed from an information system (e.g., printouts, CDs), the SP documents the specific procedures, training, and

accountability measures in place to ensure that remote use of the data does not bypass protections outlined in OMB M-06-16.

2) DHS uses PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act or in other public notices. The DHS Chief Privacy Officer 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 privacy compliance documentation such as PIAs and SORNs or other public notice(s).

3) When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act or specified in a notice, the Chief Privacy Officer evaluates whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, program owners review, update, and republish their PIAs, 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. Refer to the following documents for additional information and policies on protecting PII and Sensitive PII at DHS:

   a) *DHS Policy Directive 4300A, "Information Technology System Security Program (ITSSP), Sensitive Systems," Attachment S* "Compliance Framework for Privacy Sensitive Systems"

   b) *DHS 4300A* Policy Directive Attachment S: "Managing Computer- Readable Extracts (CRE) Containing Sensitive PII." In addition, see this Directive for PII auditing requirements and remote access requirements.

(PS) Personnel Security Control Family

DHS information systems face threats from many sources, including the actions of people (e.g., employees, external users, and contractor personnel). The intentional and unintentional actions of these individuals can potentially harm or disrupt information systems and their facilities. These actions can result in the destruction or modification of the data being processed, denial of service to the end users, and unauthorized disclosure of data, potentially jeopardizing DHS's mission.

Security is inherently a government responsibility. Contractors, others working on behalf of DHS, and other sources may assist in the performance of security functions, but a DHS employee is always designated as the responsible agent for all security requirements and functions. This section outlines the roles and responsibilities for implementing these

requirements.

DHS's personnel security requirements, at a minimum, shall:

1. Ensure that individuals occupying positions of responsibility within DHS (including third-party service providers) are trustworthy and meet established security criteria for those positions.

   a. DHS Components ensure that the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position sensitivity levels.

      i) DHS Components ensure that any Federal employee granted access to any DHS system has a favorably adjudicated Tier 2 Investigation (formerly Moderate Risk Background Investigation [MBI]) as defined in DHS Instruction 121-01-007-01, Revision 01, The Department of Homeland Security Personnel Security, Suitability and Fitness Program. In cases where non-DHS Federal employees have been investigated by another Federal agency, DHS Component personnel security organizations may, whenever practicable, use these investigations to reduce investigation requests, associated costs, and unnecessary delays). Active-duty United States Coast Guard (USCG) and other personnel subject to the Uniform Code of Military Justice (UCMJ) are exempt from this requirement.

      ii)DHS Components ensure that contractor personnel are not granted access to DHS systems without having a favorably adjudicated Background Investigation (BI) as defined in Department of Homeland Security Acquisition Regulation (HSAR) and the DHS Instruction 121-01-007-01, Revision 01, *The Department of Homeland Security Personnel Security, Suitability and Fitness Program*, Chapter 3, Federal Suitability, Excepted Service, and Contractor Employee Fitness Requirements. In cases where contractor personnel have been investigated by another federal agency, DHS Component personnel security organizations may, whenever practicable, use these investigations to reduce investigation requests, associated costs, and unnecessary delays . DHS Components ensure that no temporary employee is granted access to any DHS system without having met the review and investigation standard defined in DHS Instruction 121-01-007-01, Revision 01, *The Department of Homeland Security Personnel Security, Suitability and Fitness Program*

2. DHS Components ensure that only United States (U.S.) Citizens are granted access to DHS systems and networks. Exceptions to the U.S. Citizenship requirement are requested by submitting a completed Foreign National Visitor Access Request (VAR)

form for each foreign national to the DHS Office of the Chief Security Officer (OCSO), in accordance with this policy, Requests for Exception to U.S. Citizenship Requirement.

a. Any person of dual citizenship (one being U.S. citizenship) and any Legal Permanent Resident who requires access to DHS systems as a validated representative of foreign power is processed as indicated in this section.
b. Requests for exception to U.S. citizenship requirement: Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. citizens. Under normal circumstances, only U.S. citizens are allowed access to DHS systems and networks; but there is a need at times to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to citizenship requirements are treated differently from security policy waivers.
c. Exceptions to the U.S. citizenship requirement are requested by completing DHS Form 11059, Foreign National Employee/ Detailee/ Scientist/Student Worksheet which is available online or through the DHS OCSO, Center for International Safety & Security (CISS).
    i) Foreign Access Coordinators, in coordination with the DHS OCSO/CISS, conduct an assessment of the risk of granting the foreign nominee access to DHS systems and provide a recommendation to the DHS CISO and the respective Component CISO regarding the approval or disapproval of the request.
    ii) Foreign nationals who are provided email access will have the distinguishing email address identifier of "(FO)" for Foreign Official.
    iii) DHS HQ or Components requesting the issuance of DHS IT equipment to a foreign national will ensure the foreign national's citizenship is known to the servicing DHS HQ or Component OCIO element.
    iv) Foreign nationals nominated for access to DHS IT systems in a remote fashion, without being physically located in a DHS facility or co-located with DHS personnel (e.g., HSIN, US CERT Portal, etc.) will be submitted directly into ISMS/FAMS without the use of DHS Form 11059.
d. Hosting DHS HQ or Components select a Foreign Access Coordinator to be the point of contact to the DHS OCSO/CISS for processing requests for exception to the U.S. Citizenship policy requirement.
    i) The hosting DHS HQ or Component notifies DHS OCSO/CISS of the selected Foreign Access Coordinator.
e. DHS OCSO/CISS will require a Foreign Access SP in cases where foreign nationals will have prolonged, continuous access to DHS systems and personnel, and will request an evaluation of the physical location of foreign national assignment for inadvertent exposure to other DHS systems or information they are not authorized to

access.

f. DHS Components must submit a foreign national screening request in the Foreign Access Management System (FAMS), a module of the DHS OCSO Integrated Security Management System's (ISMS) and upload the DHS Form 11059 along with a clear, legible copy of the foreign national's passport. The results of the screening process will be shared with the DHS CISO, the respective Component CISO, and the DHS PIV Card Issuer (PCI) for DHS PIV Card enrollment and issuance. For further information regarding the citizenship exception process, contact the DHS OCSO/CISS at FAM.Support@hq.dhs.gov.

g. Exceptions to the U.S. Citizenship requirement are requested by submitting a completed DHS Form 11059 to the DHS OCSO/CISS for each foreign national requiring access to DHS systems and networks. The DHS Form 11059 constitutes a pre-systems access security review by which a foreign national's proposed access is evaluated. This security review will also address the issuance of DHS IT equipment, such as laptop and cellular telephone.

h. Refer to DHS Policy Directive 121-08, *Requirements for Security Review of Foreign National Assignments and Overseas Employment*, for further information on long-term foreign access security protocols.

1) Ensure that DHS's information and information systems are protected during and after personnel actions such as terminations and transfers.

2) DHS Components implement procedures to ensure that system access is revoked for DHS employees, contractors, or others working on behalf of DHS who leave the Component, are reassigned to other duties, or no longer require access.

3) DHS Components establish procedures to ensure that all DHS property and assets related to information systems are recovered from the departing individual and that sensitive information stored on any media is transferred to an authorized individual.

4) Employ formal sanctions for personnel failing to comply with DHS security policies and procedures.

5) Assign position risk categorizations or designations to all personnel positions held within DHS.

6) DHS Components designate the position sensitivity level for all Government and contractor positions that use, develop, operate, or maintain information systems and determine risk levels for each contractor position. Position sensitivity levels are reviewed annually and revised as appropriate. Screen users prior to authorizing access to DHS systems.

7) Users report lost, stolen, or inadvertently destroyed DHS PIV Cards to the DHS PCI by email at OneCardSDD@hq.dhs.gov and to the Component's IT Help Desk, which supplies a temporary logon.

8) Users report forgotten or misplaced PIV cards to the Help Desk, who supply a temporary logon that expires 24 hours after creation. Users also report to the DHS PCI by email at OneCardSDD@hq.dhs.gov.

(PE) Physical and Environmental Protection Control Family

Physical and environmental protection controls provide measures for DHS's system operational environment so that DHS systems are physically protected from threats and that an appropriate operating environment is provided. The broad scope of requirements includes physical access authorizations and access control of DHS's users and visitors, access control of communications and output devices (monitors, printers), and monitoring of access. Protections of the operating environment include protection of power equipment and power cabling, maintenance and repair, and management of emergency power, lighting, fire protection, temperature and humidity, water damage protection, and alternate worksites.

DHS's physical and environmental protection requirements, at a minimum, shall:

1) Limit physical access to information systems, equipment, and the respective operating environments to authorized users.
   a) Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data is limited to authorized personnel.
      i) DHS Components authorize, monitor, control and maintain records of the delivery and removal of hardware and software that enters and exits a facility.
      ii) DHS Components ensure that neither personally owned wireless mobile devices nor Government-owned wireless mobile devices are permitted in conference rooms or secure facilities where classified information is discussed. Wireless mobile devices and accessories are prohibited in areas where unclassified, sensitive information is discussed, maintained, or distributed unless specifically authorized in writing by the AO(s) for the system(s) used in the area. For additional requirement details see NIST SP 800-124, *Guidelines for Managing the Security of Mobile Devices in the Enterprise, and DHS Policy Directive 4300A, ITSSP, Sensitive Systems," Attachment I, "Mobile Devices.*"
      iii) Visitor
         (1) For definition please see the DHS Lexicon.
         (2) The visitor is placed in one of two (2) categorizes, either escort required, or no escort required. Escort required visitors are escorted at all times. No escort required visitors are granted limited general access to the facility without an escort. Escort procedures for classified areas are indicated in DHS MD 11051, SCIF Escort Procedures. (Source: DHS Lexicon)
         (3) Visitors sign in upon entering DHS facilities that house information systems,

equipment, and data. They are escorted during their stay and sign out upon leaving. Access by non-DHS contractors or vendors is limited to those work areas requiring their presence. Per National Archives and Records Schedule (GRS) 18, Item 17, Visitor Control Files. Registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers. Item 17.a. For areas under maximum security. Destroy five (5) years after final entry or five (5) years after date of document, as appropriate. Item 17.b. For other areas. Destroy two (2) years after final entry or two (2) years after date of document, as appropriate.

b) Employ security at an alternate work site that is commensurate with the security categorization level of the information processed and that supports an organizational risk assessment.
c) Assess as feasible, the effectiveness of security controls at alternate work sites.
d) Provide a means for employees to communicate with information security personnel in case of security incidents or problems.

2) Protect the physical plant and support infrastructure for information systems.
   a) Protect power equipment and power cabling for the information systems from damage and destruction.
   b) Provide capability to shut off power to the information system or individual system Components in emergency situations.
   c) Place emergency shutoff switches or devices to facilitate safe and easy access for personnel.
   d) Protect emergency power shutoff capability from unauthorized activation.
   e) Provide a short-term uninterruptible power supply to facilitate either an orderly shutdown of the information system or a transition of the information system to long-term alternate power in the event of a primary power source loss.
   f) Components control physical access to transmission medium that transmits unencrypted data within Component facilities using safeguards approved by the DHS NOSC.
3) Provide supporting utilities for information systems.
4) Protect information systems against environmental hazards.
   a) Employ and maintain 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.
   b) Employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.
   c) Maintain and monitor temperature and humidity levels within the facility where information systems reside.
   d) Protect information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.
5) Provide appropriate environmental controls in DHS facilities containing information systems.

a) Controls for deterring, detecting, restricting, and regulating access to sensitive areas are in place and sufficient in nature to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.
b) Controls are based on the level of classification and risk, determined in accordance with Departmental security policy as reflected in this and other relevant documents.
c) These requirements extend to DHS assets located at non-DHS facilities or non- DHS assets and equipment that host DHS data.
    i) Devices are transported and stored securely at all times.
d) Components control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

(PL) Planning Control Family

The objective of system security planning is to improve protection of information system resources. All DHS systems have some level of sensitivity and require protection as part of security management practices. The protection of a system must be documented in a security and privacy plan. The purpose of the security and the privacy plan is to provide an overview of the security and privacy requirements of the system and describe the controls in place or planned for meeting those requirements.

The security and privacy plan also delineate responsibilities and expected behavior of all users who access DHS systems. Implementation information can often be found in specific NIST publications, such as NIST SP 800-53.

Since the security and privacy plan establishes and documents the security and privacy controls, it should form the basis for the authorization, supplemented by the assessment report and the POA&Ms.

DHS's planning policy requirements, at a minimum, shall:

1) Develop, document, periodically update, implement System Security Plans (SSP) that describe the security controls in place or planned for the information systems, and periodically review SSP documentation during annual assessments of DHS information systems part of the Ongoing Authorization process.
    a) Information Security Program
        i) The DHS Information Security Program provides a baseline of policies, procedures, standards, and guidelines for DHS Components.
            (1) This Policy Directive provides direction to managers and senior executives for managing and protecting sensitive systems.
            (2) It also defines policies relating to management, operational, and technical

controls necessary for ensuring confidentiality, integrity, availability, authenticity, and nonrepudiation in DHS information system infrastructure and operations.

(3) The policy elements expressed in this Directive are designed to be broad in scope to accommodate the diverse operating environments.

(4) Each DHS Component is responsible for identifying, developing, and implementing any additional policies needed to meet their specific requirements.

(5) The DHS Enterprise Services Security Working Group (ESSWG) ensures the development, review and vetting of proposed security documents for current and proposed enterprise service solutions and service offerings. It also provides recommendations to the CISO Council for review and approval. The ESSWG is chaired by the DHS CISO, the DHS Headquarters CISO, and Executive Director of Enterprise Systems Development Office or their delegates.

ii) Basic Requirements

(1) Basic security management principles are followed in order to ensure the security of DHS information resources. These principles are applicable throughout the Department and form the cornerstone of the DHS Information Security Program.

(2) DHS Component CISOs and ISSMs submit all security reports concerning DHS systems to the Component senior official or designated representative. DHS Component CISOs/ISSMs interpret and manage DHS security policies and procedures to meet Federal, Departmental, and Component requirements. DHS Component CISOs/ISSMs also answer data queries from the DHS CISOD and develop and manage information security guidance and procedures unique to DHS Component requirements.

(3) An ISSO is designated for every information system and serves as the Point of Contact (POC) for all security matters related to that system. The ISSOs are the primary points of contact for the information systems assigned to them. They develop and maintain SSPs and are responsible for overall system security.

(4) The System Owner or designee develops and maintains a SSP for each information system. Component AO review and approve SSPs.

(5) The CISOD Director responsible for Policy chairs or appoints the chair for the Security Policy Working Group. The DHS Security Policy Working Group is established to promote collaboration between the Components and Headquarters in the maintenance of DHS information security policy.

(a) Each Component CISO appoints a technical Cybersecurity Subject Matter Expert representative to the DHS Security Policy Working Group

(b) The DHS Security Policy Working Group chair ensures that a report on

representative attendance is made available to Component and Department CISOs. Please see the DHS Security Policy Working Group plan for governance for additional details on the process for updating Directive 4300A.

2) Develop, document, and periodically update the rules of behavior (to include data handling rules for both PII and non-PII data) for DHS users requiring access to DHS information systems. DHS users are required to sign rules of behavior prior to being granted system accounts or access to DHS systems or data. The rules of behavior contain a "Consent to Monitor" provision and an acknowledgement that the user has no expectation of privacy.

   Rules of Behavior include, but are not limited to:

   a) Workstation Use:
      i) Components configure workstations to either log off, or activate a password-protected lock, or password-protected screensaver after 15 minutes of user inactivity for workstation activity. Users either log off or lock their workstations when unattended.
   b) Telephone Communications:
      i) Components develop guidance for discussing sensitive information over the telephone. Guidance is approved by a senior DHS Component official and is subject to review and approval by the DHS CISOD. Under no circumstances is classified national security information discussed over unsecured telephones.
      ii) Sensitive information is neither communicated over nor stored in voice mail.
   c) Use of Add on Devices
      i) The use of add-on devices, such as cameras and video/voice recorders, is not authorized unless approved by the AO. Functions that can record or transmit sensitive information via audio, video, Infrared (IR), or Radio Frequency (RF) are disabled or powered off in areas where sensitive information is discussed.
   d) Use of Personal Devices and Software
      i) DHS government and contractor personnel cannot use personal computers, phones, electronic devices, or software without the express prior written permission of the DHS CIO (DHS AO).
   e) Wireless Tactical Systems
      i) Wireless tactical systems include Land Mobile Radio (LMR) subscriber devices, infrastructure equipment, remote sensors, and technical investigative communications systems. Because they are often deployed when officer safety and mission success are at stake, wireless tactical systems require even greater security measures.
      ii) To ensure secure tactical communications, DHS Components implement strong identification, authentication, and encryption protocols designed

specifically for each wireless tactical system.

iii) Wireless tactical system policy and procedures are described more completely in Attachment M "Sensitive Wireless Tactical Systems" of the *DHS Policy Directive 4300A, "Information Technology System Security Program (ITSSP), Sensitive Systems."*

f) Radio Frequency Identification

i) Because of the computing limitations of RFID tags, it often is not feasible to implement many of the security mechanisms, such as cryptography and strong authentication, that are commonly supported on personal workstations, servers, and network infrastructure devices. RFID security controls can support Departmental and DHS Component privacy objectives, mitigate risks to business processes, and prevent the disclosure of sensitive information.

ii) DHS Components develop a contingency plan, such as the use of a fallback identification technology, to implement in case of an RFID security breach or system failure.

iii) RFID procedures are described in "Sensitive RFID Systems," Attachment L to DHS Policy Directive 4300A.

g) Use of Social Media:

i) The DHS Office of Public Affairs publishes Terms of Service (TOS) agreements and guidelines for posting to these sites. In some cases, the Department enters into its own TOS, and in other cases it endorses those of other Federal agencies such as the General Services Administration (GSA) or Office of Personnel Management (OPM).

ii) Posted content is in alignment with the Department's TOS and guidelines for a given social media host (e.g., YouTube, Twitter). This condition is also met if the Department endorses another appropriate Federal agency's guidance or TOS (e.g., GSA, OPM).

h) Use of Email and Internet Services:

i) Limited personal use of DHS email and Internet services is authorized for DHS employees as long as this use does not interfere with official duties, inhibit the security of information and information systems, or cause degradation of network services. Specifically prohibited activities include streaming of audio or video, social networking, peer-to-peer networking, software or music sharing/piracy, online gaming, Webmail, Instant Messaging (IM), hacking, and the viewing of pornography or other offensive content. DHS users comply with the provisions of DHS MD 4500.1, DHS Email Usage, and DHS Directive 262-04, DHS Web Internet and Extranet Information.

i) DHS employees may use Government office equipment and DHS systems/computers for authorized purposes only. "Authorized use" includes limited personal use as described in DHS MD 4600.1, *Personal Use of*

Government Office Equipment, and DHS MD 4900, *Individual Use and Operation of DHS Information Systems/Computers.*

ii) Contractors, others working on behalf of DHS, or other non-DHS employees are not authorized to use Government office equipment or information systems/computers for personal use, unless limited personal use is specifically permitted by the contract or memorandum of agreement. When so authorized, the limited personal use policies of this section and the provisions of DHS MD 4600.1, DHS MD 4900, DHS MD 4500.1, and DHS Directive 262-04 apply.

3) Individual accountability is a cornerstone of an effective security policy. Component Heads are responsible for taking corrective actions whenever security incidents or violations occur and for holding personnel accountable for intentional violations. Each Component determines how to best address each individual case.

j) Develop security and privacy architecture for DHS information systems and strategically allocate security safeguards (procedural, technical, or both) in the architecture so that adversaries must overcome multiple safeguards to achieve their objective.

k) Select control baselines for each DHS system and tailor them by applying specified tailoring actions in accordance with NIST FIPS 199 Security Impact Categorization requirements.

l) DHS Component information security programs are structured to support DHS and applicable FISMA 2014, OMB, and other Federal requirements. FISMA *URL: Federal Information Security Modernization Act of 2014, Public Law 113-283*

a) NIST SP 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." All uses of cloud computing by DHS follow DHS security authorization processes and procedures to include a completed security authorization package and an ATO signed by the appropriate Authorizing Official. All DHS cloud systems and services which are subject to FedRAMP requirements to use the FedRAMP process required by OMB. Organizations also review the DHS Privacy Policy for applicability in cloud environments if they are dealing with privacy data.

4) Develop, document, and periodically update policies around the procurement and use of cloud systems, services, following existing DHS security authorization processes requirements and procedures to include completing a security authorization package and an ATO signed by the Component or DHS-designated AO.

a) The Federal CIO Memorandum, *Security Authorization of Information Systems in Cloud Computing Environments*, issued on December 8, 2011, established FedRAMP to provide a cost-effective risk-based approach for the adoption and use of cloud services. For additional requirement details and guidelines, see the NIST SP 800-145, *NIST Definition of Cloud Computing*, September 2011, and the DHS SAG.

i) All DHS cloud systems and services not exempt from FedRAMP use appropriate FedRAMP documentation templates, are assessed using the Joint Authorization Board

(JAB)- approved security-control baselines and additional DHS requirements and are categorized in the FISMA inventory as either a GSS or MA. DHS cloud systems and services are not categorized as External Information Systems (EIS).

ii) All DHS cloud services of FIPS Moderate categorization or higher, consumed by or intended to be consumed by multiple government organizations outside of DHS, submit to FedRAMP for JAB Provisional Authorization.

iii) All DHS cloud systems and services are to adhere to FedRAMP process and security authorization requirements when initiating, reviewing, granting, and revoking risk assessments and security authorizations.

b) Components should leverage cloud services with FedRAMP Provisional Authority to Operate (P-ATO) whenever available when authorizing cloud systems or services. When a FedRAMP P-ATO is not available, Components may leverage, or sponsor FedRAMP compliant Agency ATO packages whenever available.

i) Components who leverage FedRAMP P-ATO Cloud Services must review the continuous monitoring (ConMon) monthly 1-pager reports, provided by the FedRAMP Program Management Office (PMO) to the agency ISSO in the Cloud Service Providers (CSP's) public facing folder, as the FedRAMP Program maintains these systems as a part of their ongoing P-ATO Authorization.

ii) Components who are leveraging FedRAMP Agency Authorized Systems, FedRAMP P-ATO Systems, or sponsor a DHS Authorization for a cloud system, are responsible for reviewing, monitoring and, or maintaining all common activities for that CSP. All DHS cloud service ATOs must follow and adhere to FedRAMP requirements. See FedRAMP Authorization Roles and Responsibilities for additional details.

(PM) Program Management Control Family

The program management policy specifies the development, implementation, assessment, authorization, and monitoring of the IT security program management. The successful implementation of security controls for DHS's data and information systems depends on the successful implementation of DHS's program management controls. As a result, the program management controls are essential for managing the IT security program.

DHS's IT security and privacy program management requirements, at a minimum, shall:

1) Develop a comprehensive strategy to manage security risk to DHS operations and assets, individuals, other organizations, and the Nation associated with the operation and use of DHS systems.

a) The DHS CISO is the authority for interpretation and clarification of the DHS Security Policy (inclusive of all Attachments and appendices).

b) The DHS CISO updates the DHS Security Policy (e.g., DHS Policy Directive *Information Technology System Security Program, Sensitive Systems*) at least annually.

2) Manage the security and privacy state of DHS systems and the environments in which those systems operate through authorization processes.
   a) The DHS Security Authorization Guide (SAG) describes detailed processes governing security authorizations. See link for additional details:
   b) DHS programs that engage in Computer Matching Agreements (CMA) follow established DHS guidance for ensuring that controls are in place to maintain both the quality and integrity of data shared under CMAs. See DHS MD 262-01 *Computer Matching Agreement and the Data Integrity Board*.
3) The DHS CISO Council and ISSMs constitute the management team responsible for ensuring the development and implementation of the DHS Information Security Program.
   a) The DHS CISO Council is responsible for implementing a security program that meets DHS mission requirements, and for reviewing specific topic areas assigned by the DHS CIO or the DHS CISOD.
   b) The DHS CISO Council is also responsible for establishing an organizational Security Strategy and Risk Management Plan; promoting communications between security programs; implementing information systems security acquisition requirements; and for developing security best practices in all enterprise and DHS Component information security programs.
      i) DHS Component CISOs actively participate in the CISO Council.
      ii) Members of the DHS CISO Council ensure that security-related decision updates to the DHS MD 140 series of security publications, are distributed to the ISSOs and other appropriate persons.
4) Implement an insider threat program that includes a cross-discipline insider threat incident handling team.
5) Develop, monitor, and report on the results of information security and privacy measures of performance.
   a) FISMA requires that the status of the DHS Information Security Program be reported to OMB on a recurring basis.
6) Implement a process to ensure that POA&Ms for the security and privacy programs and associated DHS systems are developed and maintained.
   a) Security deficiencies in any outsourced operation require creation of a program-level POA&M.
7) Implement a process for ensuring that vulnerabilities are properly identified, document remediation actions and track vulnerabilities to mitigate risk to operations, assets, individuals.
   a) See section of this 4300A document for information on POA&M Management. Additional detailed information for creating and managing POA&Ms is published in the DHS 4300A Attachment H, "Plan of Action and Milestones

(POA&M) Management Guide."

8) Develop and maintain an inventory of DHS systems.
    a) Every DHS computing resource (desktop, laptop, server, wireless mobile device, etc.) is individually accounted for as part of a FISMA Inventoried information systems.
9) DHS CFO-designated systems are systems that require additional management accountability to ensure effective internal control exists over financial reporting. For additional requirement details please see OCFO Financial Management Policy Manual.
    a) There may be additional requirements, not specific to DHS CFO designated systems, based on Appendix A to OMB Circular A-123, Management's Responsibility for Internal Controls.
    b) These requirements are in addition to both the other security requirements established in this Directive and to other system line of business (LOB) requirements developed by the CFO.
    c) These additional requirements provide a strengthened assessment process and form the basis for management's assurance of internal control over financial reporting. The strengthened process requires management to document the design and test the operating effectiveness of controls for CFO-designated systems. The System Owner is responsible for ensuring that all requirements, including security requirements, are implemented on DHS systems. DHS Component CISOs/ISSMs coordinate with their CIO and CFO organization to ensure that these requirements are implemented.
    d) The DHS CFO designates the systems that comply with additional internal controls and the Office of the CFO reviews and publish the CFO Designated System List annually. For additional details See OMB A-123 and OMB 01-02.

(RA) Risk Assessment Control Family

Risk assessment is a process to identify system security risks, determine the impact if the event occurred, and select safeguards that protect, mitigate, or eliminate this impact. This process allows Program Offices to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the information systems and information that support their organization's missions. Assessing the risks to DHS's information and information systems provides the necessary information for Program Offices and System Owners to make well-informed risk management decisions related to acceptable risk levels. The risk assessment control policies ensure that there are mechanisms in place to address the identification, assessment, and mitigation of risks to information assets.

DHS's risk assessment requirements, at a minimum, shall:

1) DHS Components establish a risk management program and process in accordance with NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, and with other applicable federal guidelines.
   a) DHS Components implement NIST SP 800-53, Revision 5, security controls, using the FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems* methodology, based on the FIPS 199 impact level high water mark established for the three separate security objectives (confidentiality, integrity, availability).
2) Periodically assess the risk to DHS operations (including mission, functions, image, or reputation), DHS assets, and individuals, resulting from the operation of DHS information systems and the associated processing, storage, or transmission of DHS information. See NIST SP 800-53, Revision 5, for details.
   a) DHS periodically assesses the selection of security controls to determine their continued effectiveness in providing an appropriate level of protection.
   b) Conduct regular risk assessments of DHS information systems.
   c) Conducting periodic e-authentication risk assessments.
   d) DHS Components through assessment authorize systems at Initial Operating Capability (IOC) and every three (3) years thereafter, or sooner, whenever a major change occurs.
   e) Upon entering the Ongoing Authorization (OA) Program, OA Components authorize systems at Initial Operating Capability (IOC), through submission of an OA Admission Letter and thereafter as needed, on a time or event driven basis in accordance with OMB A-130, NIST guidance and DHS OA Methodology.
3) Conduct periodic vulnerability assessments of DHS information systems to determine security risks that should be mitigated. See NIST SP 800-53, Revision 5, for details.

(SA) System and Services Acquisition Control Family

System and services acquisition controls ensure that appropriate technical, administrative, physical, and personnel security requirements will be included in all specifications for the acquisition, operation, and maintenance of DHS facilities, equipment, software, and related services or those operated by external providers of information system services on behalf of DHS.

DHS's system and services acquisition requirements, at a minimum, shall:

1) Allocate resources to protect DHS information systems. Employ System Development Life Cycle (SDLC) processes that incorporate information security considerations.
   a) The DHS SELC is detailed in DHS Instruction 102-01-103, *Systems Engineering Life*

Cycle.

b) Not use live data in any environment other than in production and disaster recovery (DR) environments nor use live data in development, testing or staging environments.

2) Employ software usage and installation restrictions.

3) Ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced by DHS.

a) Information security is a business driver and any risks found through security testing are ultimately business risks. Information security personnel should be involved, to the maximum extent possible, in all aspects of the acquisition process, including drafting contracts, and procurement documents. DHS MD 102-01 Rev. 3, *Acquisition Management Directive* and DHS MD 102.2, *Capital Planning and Investment Control* provide additional information on these requirements.

4) Develop information system documentation to support the configuration baseline of DHS systems.

5) DHS Components conduct reviews to ensure that information security requirements and provisions to address supply chain risk are included in contract language and that the requirements and provisions are met throughout the life of the contract.

a) All SOW, contract vehicles, and other acquisition-related documents include privacy requirements and establish privacy roles, responsibilities, and access requirements for contractors and service providers.

i) DHS requires that components preparing to purchase external, third-party, or Cloud Services to ensure ConMon Requirements are outlined in the SOW, contract requirements, the BPA, and reflected in the budget (IGCE) to make sure resources will be properly allocated to meet the requirement.

(1) Specific deliverables and tasks outlined for ConMon are specified in the Statement of Work (SOW), and/or provided in Task Orders or BPA Calls, to detail the Service Providers specific requirements.

(a) There should be sufficient labor hours budgeted in the IGCE to complete the assigned ConMon requirements by the Cloud Service Provider being contracted. Failure to provide sufficient funding may result in the contract requiring modification on the part of the DHS system owner.

(2) The BPA and, or, contract states FedRAMP Continuous Monitoring ConMon requirements, for cloud services see specific requirements outlined in the FedRAMP Cloud Service Provider Continuous Monitoring Strategy Guide which provides details about the deliverables required from FedRAMP authorized Cloud Service Providers, which includes, but is not limited, to:

(3) Monthly Vulnerability Scans.

(4) Annual Assessments as a part of the Ongoing Authorization Process.

See DHS NIST 800-53, Revision 5, control Baselines and CSAM input requirements for details.

(5) Significant Change Requests submitted for approval prior to implementation. For Cloud Services see FedRAMP SCR Requirements for details.

(6) Deviation Requests for POA&Ms and POA&M Closure evidence validation. See NIST SP 800-53r5 Schedule A for details.

(7) Incident Reporting to FedRAMP and U.S. CERT. See U.S. CERT for federal incident notification requirements and for cloud services see FedRAMP for specific incident Reporting requirements.

6) Require providers of external system services to comply with DHS's security and privacy requirements. See most current FY version of the DHS Information Security Performance Plan (ISPP).
   a) DHS requires contractors to apply information system security engineering principles in the specification, design, development, implementation, and modification of information systems, in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 Revision 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems and Federal Information Processing Standard 199 (FIPS 199) security objectives.
7) Employ DHS's supply chain safeguards to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events
   a) Procurement authorities throughout the Department enforce the provisions of the HSAR.
   b) Procurements for services and products involving facility or system access control are in accordance with DHS guidance regarding DHS HSPD-12 implementation.
8) DHS Components include requirements for software assurance and supply chain risk management prior to acquisition of any hardware or software products. Components ensure that commercial-off-the-shelf (COTS) hardware and software products in use by or being considered for use in moderate and high criticality systems, are analyzed for supply chain risk prior to acquisition activities that procure new products, upgrade existing products, or that will integrate these products with commercial services
9) Information Assurance (IA) is considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA is achieved through the acquisition and appropriate implementation of evaluated or validated COTS IA and IA-enabled IT products. These products provide for the availability of systems. The products also ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.
10) Strong preference is given to the acquisition of COTS IA and IA-enabled IT products

(to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following:

a) The NIST FIPS validation program.
b) The NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program.
c) The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement.
d) The evaluation and validation of COTS IA and IA-enabled products is conducted by authorized commercial laboratories or by NIST.

(SC) System and Communication Protection Control Family

System and communications protection controls ensure that system and communications protection policies and procedures are implemented to address the protection of information transmitted, or received by DHS information systems, to include separation of functions, cryptographic key management, denial of service, and boundary protection.

DHS's system and communication protection management requirements, at a minimum, shall:

1) Monitor, control, and protect DHS communications (e.g., information transmitted or received by DHS information systems) at the external boundaries and key internal boundaries of the information systems. See NIST SP 800-52, NIST FIPS 140-2, and NIST FIPS 140-3 for additional requirements details. See NIST SP 800-53, Revision 5, controls related to this: IA-7, SC-8, SC-8(1), SC-12, SC-13, SC-17, SC-28, and SC-28(1).
   a) Components provide adequate physical and information security for all DHS- owned Private Branch Exchanges (PBX). (Refer to NIST SP 800-24, *PBX Vulnerability Analysis*, for guidance on detecting and fixing vulnerabilities in PBX systems.)
   b) Voice over Internet Protocol (VoIP) and similar technologies move voice over digital networks. These technologies use protocols originally designed for data networking. Such technologies include Voice over Frame Relay, Voice over Asynchronous Transfer Mode, and Voice over Digital Subscriber Line (refer to NIST SP 800- 58 for additional information).
   c) DHS Components do not introduce new wireless network communications technologies into the enterprise unless the appropriate AO specifically approves a technology and application. For Wireless network communications security requirements please refer to NIST SP 800-153 for additional details.
2) Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within DHS information

systems.

a) Components shall develop a zero trust architecture plan in accordance with the requirements outlined in OMB M-22-09.

3) Separate user functionality, including user interface, from system management functionality.

4) Prevent unauthorized and unintended information transfer via shared system resources.

5) Monitor and control communications at the external boundary of DHS systems and at key internal boundaries within the system.

a) In accordance with OMB Memorandum M-15-13 and DHS Binding Operational Directive (BOD) 18-01, Components shall use HTTPS to secure HTTP traffic, including traffic that does not cross the public internet.

b) Components shall use encrypted DNS to resolve DNS queries where technically supported.

6) Where required or appropriate, all communications outside of the United States and its territories are in accordance with the Department of State Foreign Affairs Manual (FAM), 12 FAM 600, *Information Security Technology*.

7) Ensure that all external connections must be encrypted to include, but not limited to, (e.g., remote maintenance paths, external services, etc.).

8) Ensure that boundary protection between DHS and external networks is implemented by firewalls and TICs and other approved direct system interconnections.

9) Provide authentication, data integrity, data confidentiality, and non-repudiation services through cryptographic key establishment and cryptographic protection. See NIST SP 800-63-3 Digital Identity Guidelines.

a) DHS Components ensure that appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any transmission.

b) DHS Components using PKI-based encryption on any wireless device implement and maintain a key management plan approved by the DHS PKI Policy Authority See *DHS 4300A [Attachment U] PKI Instruction v2.0* for additional details.

c) DHS Components with systems requiring encryption comply with current NIST FIPS 140 encryption validation requirements. See NIST SP 800-52 and NIST FIPS 140-2 and NIST FIPS 140-3 for additional details.

(SI) System and Information Integrity Control Family

System and information integrity controls ensure that policies and procedures are implemented to protect information assets from malicious code as well as enable rapid identification, reporting, and correction of information system flaws.

The system and information integrity controls also refer to the processes and procedures used to control changes and maintain the integrity of the components for any system, including hardware and software. DHS's processes and procedures identify the configuration of

software at a given point in time, control changes to configurations systematically, maintain software integrity, provide traceability, and establish a software baseline library. This minimizes and manages risks in developing and maintaining software. Flaws in information systems provide an opportunity for systems to be compromised. Therefore, weaknesses, particularly those related to security, must be remediated through the configuration management process.

Software is vulnerable to malicious code; it is essential that DHS provide protection against malicious code and ensure mechanisms and tools are in place to assist in this protection. Too often, vulnerabilities may be embedded in spam in the form of executable programs, references to Internet addresses where malicious programs might be downloaded, or requests for personnel data from the recipient.

The system security functions are essential in the protection of DHS information assets, as it is important that these functions execute appropriately and, thus, should be verified during system startup. Information system outputs (i.e., reports, files) could be used to compromise the system or expose information that should be protected. DHS information systems must identify and handle errors by only providing the necessary information required to handle the error, limiting the information that could be used to possibly compromise the system. External security alerts and advisories provide information to personnel prior to an incident, providing a possible opportunity to correct system vulnerabilities that might potentially compromise a system.

DHS's system and information integrity requirements, at a minimum, shall:

1) Identify, report, and correct information and information system flaws in a timely manner.
2) Provide protection from malicious code at appropriate locations within DHS information systems.
    i) Wireless mobile device operation is permitted only when Component CISO - approved anti-malware software and software patches are current. Anti- malware and software patch versions approved by the Component CISO be posted in the DHS EA APL of the TRM. For additional requirement details see NIST SP 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise.

3) Monitor information system security alerts and advisories and take appropriate actions in response.
    a) DHS Components follow established procedures to ensure that sensitive information cannot be accessed or stolen by unauthorized individuals.
    b) These procedures address not only the paper (e.g., printers, faxes, etc.,) and electronic outputs from systems but also the transportation or mailing of sensitive media.

(SR) Supply Chain Control Family (Placeholder for policy in development)

Supply Chain Risk Management (SCRM) policy and procedures address the controls in the SR family as well as supply chain-related controls in other families that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of SCRM policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission-or system-specific policies and procedures.

The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to SCRM policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, EOs, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

a. DHS depends on numerous external supply chains for the hardware, software, and services needed in order to accomplish its missions effectively. Many of these supply chains are independent of one-another and come with their own set of risks. All program risk owners need to make risk management decisions on how best to manage these risks. It is often no longer enough for acquisition staff to perform due diligence at the beginning of an acquisition. Effective SCRM requires the analysis of the BIA to determine if supply chain threats represent unacceptable business or mission risk and the optimal countermeasures.
    i. A BIA is used to determine the level of risk introduced to the system by the supply chain and whether supply chain threats introduce sufficient risk to require the implementation of countermeasures.

2) Supply Chain Risk Management Plan

a. The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor

manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders. SCRM activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints and implications. It can either be standalone or incorporated into system security and privacy plans. The SCRM plan addresses managing, implementation, and monitoring of SCRM controls and the development/sustainment of systems across the SDLC to support mission and business functions.

i. DHS Components develop, document, and disseminate requirements for all programs under their control to develop a plan to address supply chain risk.
ii. DHS Components assess supply chain threats for risks associated with all hardware, software, and services acquired or projected to be acquired with the goal of mitigating those risks to the greatest extent possible.

b. Since supply chains can differ significantly across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose, and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment. SCRM plans include an expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, a description of and justification for supply chain risk mitigation measures taken, and associated roles and responsibilities. Finally, SCRM plans address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes (see SA-8).

c. Establish SCRM Team.

3) Supply Chain Controls and Processes

a. Supply chain elements include organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components. Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components. Supply chain elements and processes may be provided by organizations, system integrators, or external providers. Weaknesses or deficiencies in supply chain elements or processes represent potential vulnerabilities that can be exploited by adversaries to cause harm to the organization and affect its ability to carry out its core missions or business functions. Supply chain personnel are individuals with roles and responsibilities in the supply chain.
b. Controls that can be implemented to reduce the probability of adversaries successfully identifying and targeting the supply chain include avoiding the purchase of custom or non-standardized configurations, employing approved vendor lists with standing reputations in industry, following pre-agreed maintenance schedules and update and patch delivery mechanisms, maintaining a contingency plan in case of a supply chain event, using procurement carve-outs that provide exclusions to commitments or obligations, using diverse delivery routes, and minimizing the time between purchase decisions and delivery.
c. Controls that can be implemented to reduce the probability of adversaries successfully identifying and targeting the supply chain include avoiding the purchase of custom or non-standardized configurations, employing approved vendor lists with standing reputations in industry, following pre-agreed maintenance schedules and update and patch delivery mechanisms, maintaining a contingency plan in case of a supply chain event, using procurement carve-outs that provide exclusions to commitments or obligations, using diverse delivery routes, and minimizing the time between purchase decisions and delivery.
d. To manage supply chain risk effectively and holistically, it is important that organizations ensure that SCRM controls are included at all tiers in the supply chain. This includes ensuring that Tier 1 (prime) contractors have implemented processes to facilitate the flow down of supply chain risk management controls to sub-tier contractors. The controls subject to flow down are identified in SR-3b.

4) Provenance
   a. Every system and system component has a point of origin and may be changed

throughout its existence. Provenance is the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. Organizations consider developing procedures (see SR-1) for allocating responsibilities for the creation, maintenance, and monitoring of provenance for systems and system components; transferring provenance documentation and responsibility between organizations; and preventing and monitoring for unauthorized changes to the provenance records. Organizations have methods to document, monitor, and maintain valid provenance baselines for systems, system components, and related data. These actions help track, assess, and document any changes to the provenance, including changes in supply chain elements or configuration, and help ensure non-repudiation of provenance information and the provenance change records. Provenance considerations are addressed throughout the system development life cycle and incorporated into contracts and other arrangements, as appropriate.

b. Knowing who and what is in the supply chains of organizations is critical to gaining visibility into supply chain activities. Visibility into supply chain activities is also important for monitoring and identifying high-risk events and activities. Without reasonable visibility into supply chains elements, processes, and personnel, it is very difficult for organizations to understand and manage risk and reduce their susceptibility to adverse events. Supply chain elements include organizations, entities, or tools used for the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems and system components. Supply chain processes include development processes for hardware, software, and firmware; shipping and handling procedures; configuration management tools, techniques, and measures to maintain provenance; personnel and physical security programs; or other programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain personnel are individuals with specific roles and responsibilities related to the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of a system or system component. Identification methods are sufficient to support an investigation in case of a supply chain change (e.g., if a supply company is purchased), compromise, or event.

c. Tracking the unique identification of systems and system components during development and transport activities provides a foundational identity structure for the establishment and maintenance of provenance. For example, system components may be labeled using serial numbers or tagged using RFID tags.

Labels and tags can help provide better visibility into the provenance of a system or system component. A system or system component may have more than one unique identifier. Identification methods are sufficient to support a forensic investigation after a supply chain compromise or event.

d. For many systems and system components, especially hardware, there are technical means to determine if the items are genuine or have been altered, including optical and nanotechnology tagging, physically unclonable functions, side-channel analysis, cryptographic hash verifications or digital signatures, and visible anti-tamper labels or stickers. Controls can also include monitoring for out of specification performance, which can be an indicator of tampering or counterfeits. Organizations may leverage supplier and contractor processes for validating that a system or component is genuine and has not been altered and for replacing a suspect system or component. Some indications of tampering may be visible and addressable before accepting delivery, such as inconsistent packaging, broken seals, and incorrect labels. When a system or system component is suspected of being altered or counterfeit, the supplier, contractor, or original equipment manufacturer may be able to replace the item or provide a forensic capability to determine the origin of the counterfeit or altered item. Organizations can provide training to personnel on how to identify suspicious system or component deliveries.

e. Authoritative information regarding the internal composition of system components and the provenance of technology, products, and services provides a strong basis for trust. The validation of the internal composition and provenance of technologies, products, and services is referred to as the pedigree. For microelectronics, this includes material composition of components. For software this includes the composition of open-source and proprietary code, including the version of the component at a given point in time. Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid. The validation of the internal composition and provenance can be achieved by various evidentiary artifacts or records that manufacturers and suppliers produce during the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of technology, products, and services. Evidentiary artifacts include, but are not limited to, software identification (SWID) tags, software component inventory, the manufacturers' declarations of platform attributes (e.g., serial numbers, hardware component inventory), and measurements (e.g., firmware hashes) that are tightly bound to the hardware itself.

5) Acquisition Strategies, Tools, and Methods

a. The use of the acquisition process provides an important vehicle to protect the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the SDLC. Organizations also consider providing incentives for suppliers who implement controls, promote transparency into their processes and security and privacy practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.
b. Adversaries can attempt to impede organizational operations by disrupting the supply of critical system components or corrupting supplier operations. Organizations may track systems and component mean time to failure to mitigate the loss of temporary or permanent system function. Controls to ensure that adequate supplies of critical system components include the use of multiple suppliers throughout the supply chain for the identified critical components, stockpiling spare components to ensure operation during mission-critical times, and the identification of functionally identical or similar components that may be used, if necessary.
c. Organizational personnel or independent, external entities conduct assessments of systems, components, products, tools, and services to uncover evidence of tampering, unintentional and intentional vulnerabilities, or evidence of noncompliance with supply chain controls. These include malicious code, malicious processes, defective software, backdoors, and counterfeits. Assessments can include evaluations; design proposal reviews; visual or physical inspection; static and dynamic analyses; visual, x-ray, or magnetic particle inspections; simulations; white, gray, or black box testing; fuzz testing; stress testing; and penetration testing (see SR-6(1)). Evidence generated during assessments is documented for follow-on actions by organizations. The evidence generated during the organizational or independent assessments of supply chain elements

may be used to improve supply chain processes and inform the SCRM process. The evidence can be leveraged in follow-on assessments. Evidence and other documentation may be shared in accordance with organizational agreements.

6) Supplier Assessments and Reviews
   a. An assessment and review of supplier risk includes security and SCRM processes, foreign ownership, control or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors. The reviews may be conducted by the organization or by an independent third party. The reviews consider documented processes, documented controls, all-source intelligence, and publicly available information related to the supplier or contractor. Organizations can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits. In some cases, it may be appropriate or required to share assessment and review results with other organizations in accordance with any applicable rules, policies, or inter-organizational agreements or contracts.
   b. Relationships between entities and procedures within the supply chain, including development and delivery, are considered. Supply chain elements include organizations, entities, or tools that are used for the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems, system components, or system services. Supply chain processes include SCRM programs; SCRM strategies and implementation plans; personnel and physical security programs; hardware, software, and firmware development processes; configuration management tools, techniques, and measures to maintain provenance; shipping and handling procedures; and programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain actors are individuals with specific roles and responsibilities in the supply chain. The evidence generated and collected during analyses and testing of supply chain elements, processes, and actors is documented and used to inform organizational risk management activities and decisions.
7) Supply Chain Operations Security
   a. Supply chain operations security (OPSEC) expands the scope of OPSEC to include suppliers and potential suppliers. OPSEC is a process that includes identifying critical information, analyzing friendly actions related to operations and other activities to identify actions that can be observed by potential adversaries, determining indicators that potential adversaries might obtain that could be interpreted or pieced together to derive information in sufficient time to cause harm to organizations, implementing safeguards or countermeasures to

eliminate or reduce exploitable vulnerabilities and risk to an acceptable level, and considering how aggregated information may expose users or specific uses of the supply chain. Supply chain information includes user identities; uses for systems, system components, and system services; supplier identities; security and privacy requirements; system and component configurations; supplier processes; design specifications; and testing and evaluation results. Supply chain OPSEC may require organizations to withhold mission or business information from suppliers and may include the use of intermediaries to hide the end use or users of systems, system components, or system services.

8) Notification Agreements
    a. The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.
9) Tamper Resistance and Detection
    a. Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.
    b. Employ anti-tamper technologies, tools, and techniques throughout the SDLC.
10) Inspection of Systems or Components
    a. The inspection of systems or systems components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from organization-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.
11) Component Authenticity
    a. Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include CISA.
    b. Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policies and procedures support tamper

resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include CISA.

12) Component Disposal

a. Data, documentation, tools, or system components can be disposed of at any time during the SDLC (not only in the disposal or retirement phase of the life cycle). For example, disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, partial reuse of components. Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media, which contain sensitive or proprietary information. Additionally, proper disposal of system components helps to prevent such components from entering the gray market.

Definitions

The definitions in this section apply to the policies and procedures discussed in this Policy Directive. In general, the sources for the definitions given in this section are relevant NIST documents. Other definitions may be found in Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance Glossary," 6 April 2015. Definitions bearing on Privacy are sourced from DHS Policy Directive 140-07, "Privacy Incident Handling Guidance" and DHS MD 047-01, "Privacy Compliance" documentation issued by the DHS Privacy Office.

TERM	DEFINTION
Acceptable Risk	Mission, organizational, or program-level risk deemed tolerable by the Risk Executive after adequate security has been provided.
Adequate Security	Adequate security' means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls [OMB Circular A-130]
Administrative (Managerial) Controls	These controls focus on managing both system information security controls and system risk. These controls consist of risk mitigation techniques normally used by management.
Agency	Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.
Annual Assessment	Department of Homeland Security (DHS) activity for meeting the annual Federal Information Security Modernization Act of 2014 (FISMA) self- assessment requirement.
Assessment	The testing or evaluation of security or privacy controls 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 an information system or organization.
Authorization Package	The documents submitted to the AO for the Authorization Decision. An Authorization Package consists of: • Security Plan

TERM	DEFINTION
	• Security Assessment (SPR) Plan • Security Assessment Report (SAR) • Signed Accreditation Decision Letter/ATO • Contingency Plan (CP) • Contingency Plan Test (CPT)
Authorizing Official (AO)	An official within a Federal Government agency empowered to grant approval for a system to operate.
Availability	Ensuring timely and reliable access to and use of information.
Certification/ Certifying Agent	A contractor that performs certification tasks as designated by the CO.
Certificate Authority (CA)	A trusted third party that issues certificates and verifies the identity of the holder of the digital certificate.
Chief Information Officer (CIO)	The executive within a Federal Government agency responsible for its information systems.
Classified National Security Information	Information that has been determined, pursuant to Executive Order 13526, "Classified National Security Information," to require protection against unauthorized disclosure and is marked to indicate its classified status. [Source: Executive Order 13526]
Component	A DHS Component is any organization which reports directly to the Office of the Secretary (including the Secretary, the Deputy Secretary, the Chief of Staff's, Counselors, and staff, when approved as such by the Secretary), including both Operational Components and Support Components (also known as Headquarters Components). [Source DHS Lexicon and DHS MD 112-01]
Compensating Control	An internal control intended to reduce the risk of an existing or potential control weakness.
Computer Security Incident Response Center (CSIRC)	DHS organization that responds to computer security incidents.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

TERM	DEFINTION
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Continuity of Operations	Internal organizational efforts to ensure that a viable capability exists to continue essential functions across a wide range of potential emergencies, through plans and procedures that: • Delineate essential functions and supporting information systems • Specify succession of office and the emergency delegation of authority • Provide for the safekeeping of vital records and databases • Identify alternate operating facilities, if necessary • Provide for interoperable communications • Validate the capability to recover through tests, training, and exercises
Continuity of Operations Plan (COOP)	A predetermined set of instructions or procedures, required by Presidential Policy Directive 40, "National Continuity Programs" (PPD-40), and Federal Continuity Directive 1, "Federal Executive Branch National Continuity Program and Requirements" (FCD-1), that describes how an organization's essential functions are prioritized, and maintained, for at least 30 days following the occurrence of an emergency or until normal operations are resumed.
Controlled Unclassified Information	Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government -wide policies that adhere to Executive Order 13556 which establishes a program for managing CUI across the Executive branch to ensure compliance of CUI implementation.
Designated Approval Authority (DAA)	Obsolete term; see Authorizing Official (AO).

TERM	DEFINTION
DHS System	A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on behalf of DHS. DHS systems include general support systems and major applications. If a system is not owned or operated by DHS, and the data on that system is not owned or controlled by DHS, DHS is not responsible for ensuring that an authorization to operate is in force on that system.
Digital Signature	Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay.
Electronic Signature	The process of applying any mark in electronic form with the intent to sign a data object. See also digital signature.
Essential Functions	Essential functions are those that enable Executive Branch agencies to provide vital services, exercise civil authority, maintain the safety and wellbeing of the general populace, and sustain industrial capability and the national economy base during an emergency.
External System Service	A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security and privacy controls or the assessment of security and privacy control effectiveness.
Federal Information Security Modernization Act (FISMA)	FISMA requires each agency to develop, document, and implement an agency-wide information security program that provides a high level of security for the information and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA requires that the Chief Information Officer (CIO) designate a senior agency information security official to develop and maintain a Department-wide information security program. The designee's responsibilities include: • Developing and maintaining information security policies, procedures, and control techniques that address all applicable requirements • Training and overseeing personnel with significant information

TERM	DEFINTION
	security responsibilities • Assisting senior Department officials with respect to their responsibilities under the statute • Ensuring that the Department has sufficient trained personnel to ensure the Department's compliance with the statute and related policies, procedures, standards, and guidelines • Ensuring that the Department CIO, in coordination with other senior Department officials, reports annually to the Secretary on the effectiveness of the Department's information security program, including the progress of remedial actions
For Official Use Only (FOUO)	The marking instruction or caveat "For Official Use Only" will be used within the DHS community to identify sensitive but unclassified information that is not otherwise specifically described and governed by statute or regulation. Note: The term *sensitive information* as well as others such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) will no longer be used upon implementation of 32 CFR 2002, which will require use of the term Controlled Unclassified Information (CUI).
High Value Assets	High Value Assets refer to those assets; systems, information, information systems, and data, for which unauthorized disclosure or loss of control could cause exceptionally grave harm to the United States (U.S.). These IT resources may contain sensitive controls, instructions, data used in critical Federal operations, or unique collections of data (by size or content), or support an agency's mission essential functions, making them of specific value to criminal, politically motivated, or state-sponsored actors for either direct exploitation or to cause a loss of confidence in the U.S. Government.
Incident	An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

TERM	DEFINTION
Information and Communications Technology (ICT)	The organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers**.**
Information Security Vulnerability Management (ISVM)	A DHS system that provides notification of newly discovered vulnerabilities and tracks the status of vulnerability resolution.
Information System	Any information technology that is (1) owned, leased, or operated by any DHS Component, (2) operated by a contractor on behalf of DHS, or (3) operated by another Federal, state, or local Government agency on behalf of DHS.
Information System Security Officer (ISSO)	A Government employee or contractor who implements and/or monitors security for a particular system.
Information	Information is stimuli that has meaning in some context for its receiver. Information is created when data are processed, interpreted, organized, structured, or presented so as to make them meaningful or useful. Information provides context for data.
Information Security	Division E of the Clinger-Cohen Act of 1996 (Public Law 104-106) defines Information Technology (IT) as: "(6) Information technology—The term "information technology"— (A) with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use— (i) of that equipment; or

TERM	DEFINTION
	(ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product. (B) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but (C) does not include any equipment acquired by a federal contractor incidental to a federal contract." The term information system as used in this policy document, is equivalent to the term information technology system.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
Integrity	Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.
Least Privilege	The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
Major Application	A major application (MA) is an automated information system (AIS) that OMB Circular A-130 defines as requiring "…special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application." All Federal applications require some level of protection. Certain applications, because of the information they contain, however, require special management oversight and classification as MAs. Each MA is under the direct oversight of a Component CISO or Information System Security Manager (ISSM) and has an ISSO assigned.

TERM	DEFINTION
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. Examples include: a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of ad-ware are also examples of malicious code.
Management Controls	The security controls for an information system that focus on the management of risk and the management of information system security.
National Intelligence Information	The Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458, 118 Stat. 3662) amended the National Security Act of 1947 (50 U.S.C. 401a) to provide the following definition: ''(5) The terms 'national intelligence' and 'intelligence related to national security' refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that— (A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and (B) that involves— (i) threats to the United States, its people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security.''.
Network	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Operational Controls	These controls focus on mechanisms primarily implemented and executed by the people responsible for use of the system. Operational controls are designed to improve the security of a particular system or group of systems and often rely on management and technical controls.
Operational Data	Operational data is information used in any DHS mission activity.
Operational Risk	The risk contained in a system under operational status. It is the risk that an AO accepts when granting an ATO.

TERM	DEFINTION
Personally Identifiable Information (PII)	Any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the United States. [see also Sensitive Personally Identifiable Information]
Pilot	A test system in the production environment that may contain operational data and may be used to support DHS operations, typically in a limited way.
Policy Enforcement Point (PEP)	A firewall or similar device that can be used to restrict information flow.
Privacy Control	The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.
Privacy Plan	A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.
Policy Statement	A high-level rule for guiding actions intended to achieve security objectives.
Privacy Sensitive System	A Privacy Sensitive System is any system that collects, uses, disseminates, or maintains PII or Sensitive PII.
Production	The applications and systems that DHS end users' access and use operationally to execute business transactions.

TERM	DEFINTION
Privileged User	A user that is authorized (and, therefore, trusted) to perform security- relevant functions for purposes including but not limited to network system administration, security policy and procedure management, and system maintenance and controls. (Source: NISTIR 7298 rev 2.0
Prototype	A test system in a test environment that must not contain operational data and must not be used to support DHS operations.
Public Information	Public information can be disclosed to the public without restriction but requires protection against erroneous manipulation or alteration (e.g., public websites).
Remote Access	Access to a DHS information system by a user (or an information system) communicating through an external, non-DHS-controlled network (e.g., the Internet).
Residual Risk	The risk remaining after security controls have been applied.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Acceptance Memo	Memo drafted by the Component CISO for DHS CISOD when a component fails to fully meet compliance requirements for a POA&M or waiver, within a 12 month window as required. See Waivers in the POA&M requirements page 19, section 3 of this Policy Directive and Attachment B *Waivers and Risk Acceptance Request Form* for additional details.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Part of risk management incorporates threat and vulnerability analyses and analyses of privacy-related problems arising from information processing and considers mitigations provided by security and privacy controls planned or in place.
Risk Executive (RE)	An individual who ensures that risks are managed consistently across the organization. An RE can be at the Departmental or Component level.

TERM	DEFINTION
Risk Management	The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.
Security Assessment Plan	The security assessment plan and privacy assessment plan provide the objectives for the security and privacy control assessments, respectively, and a detailed roadmap of how to conduct such assessments. These plans may be developed as one integrated plan or as distinct plans, depending upon organizational needs. [per NIST SP 800-53A]
Security Control	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Assessor	A senior management official who certifies the results of the security control assessment. He or she is a Federal Government employee.
Security Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Security Operations Center (SOC)	The DHS Enterprise Security Operations Center (ESOC) coordinates security operations for the DHS enterprise. Each Component also has a SOC that coordinates Component security operations.
Security Policy	A set of criteria for the provision of security services.
Security Requirement	A formal statement of action or process applied to an information system and its environment in order to provide protection and attain security objectives. Security requirements for any given system are contained in its Security Plan.
Senior Agency Information Security Official (SAISO)	The point of contact within a Federal Government agency responsible for its information system security.

TERM	DEFINTION
Sensitive Information	Sensitive Information is any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. Sensitive Information includes: • Chemical-terrorism Vulnerability Information (CVI) • Protected Critical Infrastructure Information (PCII) • Sensitive Security Information (SSI) • Personally Identifiable Information (PII)
Sensitive Information	Any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. Note: The term *sensitive information* as well as others such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) will no longer be used upon implementation of 32 CFR 2002, which will require use of the term Controlled Unclassified Information (CUI).
Sensitive Personally Identifiable Information (SPII)	Sensitive Personally Identifiable Information (SPII) is a subset of PII [see definition above], which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. [see also Personally Identifiable Information]
Sensitive System	A sensitive system is any combination of facilities, equipment, personnel, procedures, and communications that is integrated for a specific purpose, and that may be vulnerable to an adversarial attack by an adversary seeking to violate or disrupt the system's confidentiality, integrity, or availability.
Significant Incident	A computer security-related incident that represents a meaningful threat to the DHS mission and requires immediate leadership notification.

TERM	DEFINTION
Software	Computer programs and associated data that may be dynamically written or modified during execution.
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
Strong Authentication	A method used to secure computer systems and/or networks by verifying a user's identity by requiring two-factors in order to authenticate (something you know, something you are, or something you have). Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multi-factor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. [See the discussion of Level 4 assurance in NIST SP 800-63-3, "Digital Identity Guidelines," (June 2017)
Supply Chain	A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. Source: CNSSI 4009
Supply Chain Risk Management	A decision-making process, usually supported by imperfect or incomplete information, undertaken for the purpose of prioritizing actions related to procuring ICT in support of the mission. Source: DHS SCRM PMO
System	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.
System Component	A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.
System Owner	The agency official responsible for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.
Technical Controls	The security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in system hardware, software, or firmware.

TERM	DEFINTION
Temporary/ Emergency Account	Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as 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, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training.
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Trust Zone	A Trust Zone consists of any combination of people, information resources, IT systems, and networks that are subject to a shared security policy (a set of rules governing access to data and services). For example, a Trust Zone may be set up between different network segments that require specific usage policies based on information processed, such as law enforcement information.
Two-Factor Authentication	The classic paradigm for authentication systems identifies three factors as the cornerstone of authentication: • *Something you know* (for example, a password or Personal Identification Number (PIN) • *Something you have* (for example, an ID badge or a cryptographic key) • *Something you are* (for example, a fingerprint or other biometric data) The strength of authentication systems is largely determined by the

TERM	DEFINTION
	number of factors incorporated by the system. Implementations that use two factors are considered to be stronger than those that use only one factor." A requirement for two of the three factors listed above constitutes two factor authentication.
Unclassified Information	Information that has not been determined to be classified pursuant to Executive Order 13526, as amended.
Usability	Usability, a measure of how easy user interfaces are to use. Usability is typically defined by five quality components, including learnability of the interface or process, efficiency of completing tasks, memorability of interface mechanisms, resistance-to-errors and user satisfaction.
USB Device	A device that can be connected to a computer via a USB port.
User	Individual, or (system) process acting on behalf of an individual, authorized to access a system.
User-Centered Design	Design processes that focus on the needs, wants, and limitations of the target audience of a product at each stage in the design process.
Visitor	A guest or temporary employee who presents themselves or is presented by a sponsor, for entry for less than 6 months to a secured facility that is not their primary work location. [Source: DHS Lexicon] The visitor is placed in one of two categorizes, either ***escort required,*** or ***no escort required***. ***Escort required*** visitors are escorted at all times. ***No escort required*** visitors are granted limited general access to the facility without an escort. Escort procedures for classified areas are indicated in DHS MD 11051 "SCIF Escort Procedures." [Source: DHS Lexicon]
Vital Records	Electronic and hardcopy documents, references, databases, and information systems needed to support essential functions under the full spectrum of emergencies.
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

TERM	DEFINTION
Vulnerability Scanning	An automated scan for potential security vulnerabilities.
Waiver	Temporary dispensation of a policy requirement granted to a Component to operate a system while working toward remediation of compliance deficiency within 12 months. See Attachment B Waiver and Risk Acceptance Request Form for additional details.

Acronyms

The acronyms in this section apply to the policies and procedures discussed in this Policy Directive. Otherwise, in general, the sources for the acronyms given in this section are relevant NIST documents, Policy Directives, and Policy Memos.

Acronym	Meaning
3DES	Triple Data Encryption Standard
3PAO	Third Party Assessors
AES	Advanced Encryption Standards
AIS	Automated Information System
A-Number	Alien Registration Number
AO	Authorizing Official
ARB	Acquisition Review Board
ASCII	American Standard Code for Information Interchange
ATO	Authority to Operate
BI	Background Investigation
BIA	Business Impact Assessment
BLSR	Baseline Security Requirements
BOD	Binding Operational Directive
CA	Certification Authority
CAC	Common Access Card
CBP	Customs and Border Protection
CCB	Change Control Board
CCE	Common Configuration Enumeration
CD	Compact Disc
CFO	Chief Financial Officer
CI	Counterintelligence
CIO	Chief Information Officer
CISID	Chief, Internal Security and Investigations Division
CISID-OIS	Chief, Internal Security and Investigations Division, Office of Security
CISO	Chief Information Security Officer
CM	Configuration Management
CMA	Computer Matching Agreements
CMG	Core Management Group
CMP	Configuration Management Plan
CNSS	Committee on National Security Systems

Acronym	Meaning
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan Continuity of Operations Planning
COTS	Commercial-off-the-shelf
CP	Contingency Plan Contingency Planning
CPE	Common Platform Enumeration
CPIC	Capital Planning and Investment Control
CRE	Computer-Readable Extract
CRL	Certificate Revocation List
CSO	Chief Security Officer
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNSSEC	Domain Name System Security Extensions
DOD	Department of Defense
EA	Enterprise Architecture
EAB	Enterprise Architecture Board
ED	Executive Directive
EMSG	Email Security Gateway
EO	Executive Order
EOC	Enterprise Operations Center 2,
ESSA	Enterprise System Security Agreement
ESSWG	Enterprise Services Security Working Group
EV	Extended Validation
FAM	Foreign Affairs Manual
FBCA	Federal Bridge Certification Authority
FDCC	Federal Desktop Core Configuration
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FICAM	Federal Identity, Credentialing, and Access Management

Acronym	Meaning
FIPS	Federal Information Processing Standard
FIPPS	Fair Information Practice Principles
FISMA	Federal Information Security Modernization Act of 2014
FLETC	Federal Law Enforcement Training Center
FNVMS	Foreign National Vetting Management System
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FPKI	Federal Public Key Infrastructure
FPKI PA	Federal PKI Policy Authority
FTP	File Transfer Protocol
FYHSP	Future Years Homeland Security Program
GPEA	Government Paperwork Elimination Act
GSA	General Services Administration
GSS	General Support System
HQ	Headquarters
HSAR	Homeland Security Acquisition Regulations
HSDN	Homeland Secure Data Network
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation and Air Conditioning
I&A	Intelligence and Analysis
IA	Identification and Authentication Information Assurance
IACS	Information Assurance Compliance System
IATO	Interim Authority to Operate
ICAM	Identity, Credentialing, and Access Management
ICCB	Infrastructure Change Control Board
ICE	Immigration and Customs Enforcement
IDS	Intrusion Detection System
IOC	Initial Operating Capability
IPS	Intrusion Prevention System
IPT	Integrated Project Team
IR	Infrared
IRB	Investment Review Board
ISA	Interconnection Security Agreement

Acronym	Meaning
ISMS	Integrated Security Management System
ISO	Information Security Office
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISVM	Information System Vulnerability Management
IT	Information Technology
JAB	Joint Authorization Board
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LE	Law Enforcement
LMR	Land Mobile Radio
MA	Major Application
MBI	Moderate Risk Background Investigation
MD	Management Directive
MMS	Multimedia Messaging Service
NARA	National Archives and Records Administration
NCCIC	National Cybersecurity and Communications Information Center
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NPPD	National Protection and Programs Directorate
NPE	Non-person Entity
NSA	National Security Agency
NSS	National Security System(s)
NTP	Network Time Protocol
OA	Ongoing Authorization
OCIO	Office of the Chief Information Officer
OCSO	Office of the Chief Security Officer
OCSP	Online Certificate Status Protocol
OID	Object identifier
OIG	Office of Inspector General
OIMO	Organization Identity Management Official
OMB	Office of Management and Budget
OPA	Office of Public Affairs

Acronym	Meaning
OPM	Office of Personnel Management
ORMB	Operational Risk Management Board
OTAR	Over-The-Air-Rekeying
PA	Policy Authority
PAdES	PDF Advanced Electronic Signatures
P-ATO	Provisional Authority to Operate
PBX	Private Branch Exchange
PCI	PIV Card Issuer
PCS	Personal Communications Services
PDVAL	Path Development and Validation
PEP	Policy Enforcement Point
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identity Number
PIRT	Privacy Incident Response Team
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification - Interoperable
PKI	Public Key Infrastructure
PKI PA	PKI Policy Authority
PKI MA	PKI Management Authority
PM	Program Manager
PMA	Policy Management Authority
PMO	Program Management Office
PNS	Protected Network Services
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPOC	Privacy Point of Contact
PSTN	Public Switched Telephone Network
PTA	Privacy Threshold Analysis
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFID	Radio Frequency Identification
~~RMS~~	~~Risk Management System~~ Term superseded by IACS
RMF	Risk Management Framework
RPS	Principal Certification Authority

Acronym	Meaning
S&T	Science and Technology [Component of DHS]
SA	Security Architecture
SAISO	Senior Agency Information Security Officer
SAN	Subject Alternative Name
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SCAP	Security Content Automation Protocol
SCI	Sensitive Compartmented Information
SCRM	Supply Chain Risk Management
SELC	Systems Engineering Life Cycle
SEN	Security Event Notification
SLA	Service Level Agreement
SME	Subject Matter Expert
SMS	Short Message Service
SOA	Service Oriented Architecture
ESOC	Security Operations Center
SORN	System of Records Notice
SOW	Statement of Work
SP	Special Publication Security Plan
SSH	Secure Shell
SSL	Secure Socket Layer
SSP	Shared Service Provider
Stat.	Statute (refers to a law found in *U.S. Statutes at Large*)
STE	Secure Terminal Equipment
~~TAF~~	~~Trusted Agent FISMA~~ Term superseded by IACS
TFPAP	Trust Framework Provider Adoption Process
TIC	Trusted Internet Connections
TLS	Transport Layer Security
TOS	Terms of Service
TRAL	Trigger Accountability Log
TRM	Technical Reference Model
TS	Top Secret
TS/SCI	Top Secret, Sensitive Compartmented Information
TSA	Transportation Security Administration

Acronym	Meaning
UCMJ	Uniform Code of Military Justice
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Service
USGCB	U.S. Government Configuration Baseline
USSS	United States Secret Service
VAT	Vulnerability Assessment Team
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
XML	Extended Markup Language

Authorities and References

DHS established a department-wide information security policy based on the following EOs, DHS MDs and policies, public laws and regulations, and national policies:

A. Clinger-Cohen Act of 1996, Public Law 104-106
B. CNSSI 1001, "National Instruction on Classified Information Spillage," June 2021
C. CNSSI 4009, "Committee on National Security Systems (CNSS) Glossary," April 2015
D. Computer Fraud and Abuse Act of 1986, Public Law 99-474, 100 Stat. 1213
E. Department of Homeland Security Acquisition Manual, October 2009
F. Department of Homeland Security Acquisition Regulation, May 2021
G. DHS MD 102-01, "Acquisition Management Directive," February 2019
H. DHS MD 139-05, "Accessible Systems and Technology Program," November 2018
I. DHS MD 140-01, "Information Technology Security Program," May 2017
J. DHS MD 142-03, "Electronic Mail Usage and Maintenance," January 2018
K. DHS MD 1030, "Corrective Action Plans," May 2006
L. DHS MD 4600.1, "Personal Use of Government Office Equipment," April 2003
M. DHS MD 4900, "Individual Use and Operation of DHS Information Systems/Computers"
N. DHS MD 11042.1, "Safeguarding Sensitive But Unclassified (For Official Use Only) Information," January 2005
O. E-Government Act of 2002, Public Law 107-347, 116 Stat. 2899, 44 U.S.C. 101
P. Electronic Signatures in Global and National Commerce Act (E-Sign Act), 15 U.S.C. §7001, Public Law 106-229, June 2000
Q. Executive Order 13526 of December 29, 2009, Classified National Security Information
R. Executive Order 13556 of November 4, 2010, Controlled Unclassified Information
S. Executive Order 13800 of May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
T. Federal Cybersecurity Workforce Assessment Act of 2015, Public Law 114-113 (Title III and IV)
U. Federal Information Security Modernization Act of 2014, Public Law 113-283, 128 Stat. 3073
V. Freedom of Information Act of 2002, as amended, 5 U.S.C. 552, Public Law 93-579
W. Freedom of Information Act Improvement Act of 2016, as amended, 5 U.S.C. 552, Public Law 114-185
X. GAO, "Federal Information System Controls Audit Manual (FISCAM)," February 2009
Y. Government Paperwork Elimination Act (GPEA), Public Law 105-277, October 1998
Z. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191
AA. Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," December 2003
BB. Homeland Security Presidential Directive 12, "Policy for Common Identification Standard for Federal Employees and Contractors," August 2004
CC. Intelligence Community Directive (ICD) 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," September 2008
DD. Intelligence Reform and Terrorism Act of 2002, as emended, 5 U.S.C. 552, Public Law 93-579

EE. Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, 118 Stat. 363
FF. National Archives and Records Administration (NARA) General Records Schedule (GRS) 4.2: Information Access and Protection Records, April 2020
GG. NARA GRS 5.3: Continuity and Emergency Planning Records, April 2020
HH. NARA GRS 5.6: Security Records, April 2020
II. Paperwork Reduction Act of 1995, Public Law 104-13
JJ. Privacy Act of 1974, as amended, 5 U.S.C. §552a, Public Law 93-179
KK. Records Management by Federal Agencies, 44 U.S.C. 31
LL. Section 508 of the Rehabilitation Act of 1973 (Rehab Act)
MM. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) of 2001, Public Law 107-56
NN. 5 Code of Federal regulations (CFR) §2635, Office of Government Ethics, "Standards of Ethical Conduct for Employees of the Executive Branch"

OMB Guidance:

A. Appendix III to OMB Circular No. A-130, "Security of Federal Automated formation Resources"
B. OMB Bulletin 21-04, "Audit Requirements for Federal Financial Statements," June 11, 2021
C. OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," December 2016
D. OMB Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," July 15, 2016
E. OMB Circular No. A-130, "Managing Information as a Strategic Resource," July 2016
F. OMB Memorandum M-01-05, "Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy," December 2000
G. OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 2003
H. OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information," May 2006
I. OMB Memorandum M-06-16, "Protection of Sensitive Agency Information," June 2006
J. OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 2007
K. OMB Memorandum M-09-02, "Information Technology Management Structure and Governance Framework," October 2008
L. OMB Memorandum 10-28, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)," July 2010
M. OMB Memorandum 11-06, "WikiLeaks - Mishandling of Classified Information," November 2010
N. OMB Memorandum 12-20, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," September

2012

O. OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 2003
P. OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 2003
Q. OMB Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors," August 2005
R. OMB Memorandum M-16-17, "OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control," July 2016
S. OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 2017
T. OMB Memorandum M-17-25, "Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 2017
U. OMB Memorandum M-18-16, "Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk," June 2018
V. OMB Memorandum M-19-03, "Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program," December 2018
W. OMB Memorandum M-19-17, "Enabling Mission Delivery through Improved Identity, Credential, and Access Management," May 2019
X. OMB Memorandum M-20-04, "Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements," November 2019
Y. OMB M-19-26, "Update to the Trusted Internet Connections (TIC) Initiative," September 12, 2019.
Z. OMB M-20-32 "Improving Vulnerability Identification, Management, and Remediation," September 2, 2020.
AA. OMB Memorandum M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," August 2021
BB. OMB M-22-05 Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements" December 6, 2021
CC. OMB M-22-09 "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," January 26, 2022.
DD. OMB M-22-01 "Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response," October 8, 2021.
EE. OMB M-21-31 "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident," August 27, 2021.
FF. OMB "M-21-30 Protecting Critical Software Through Enhanced Security Measures," August 10, 2021.

NIST Guidance:

A. "Framework for Improving Critical Infrastructure Cybersecurity," April 2018
B. NIST FIPS, including:
   i. NIST FIPS 140-3, "Security Requirements for Cryptographic Modules," March 2019
   ii. NIST FIPS 199, "Standards for Security Categorization of Federal

Information and Information Systems," February 2004

iii. NIST FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006

iv. NIST FIPS 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013

v. NIST FIPS 201-3, "Personal Identity Verification (PIV) of Federal Employees and Contractors," DRAFT January 2022

vi. NIST FIPS 202, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, " August 4, 2015

vii. NIST FIPS 186-4, "Digital Signature Standard (DSS)," July 2013

viii. NIST FIPS 186-5, "Digital Signature Standard (DSS), " DRAFT October 2019

C. NISTR 7298, Revision 3, "Glossary of Key Information Security Terms," July 2019

NIST SP 800 Series, including:

A. NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems," February 2006

B. NIST SP 800-16, "Information Technology Security Training Requirements: A Role-and Performance-Based Model," April 1998

C. NIST SP 800-16, Revision 1, "Information Technology Security Training Requirements: A Role-and Performance-Based Model," DRAFT April 30, 2014

D. NIST SP 800-30, Revision 1, "Guide for Conducting Risk Assessments," September 2012

E. NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems," May 2010 (Updated November 2010)

F. NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations," December 2018

G. NIST SP 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View", March 2011

H. NIST SP 800-50 Revision 1, "Building an Information Technology Security Awareness and Training Program," September 21, 2021

I. NIST SP 800-52, Revision 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations," August 2019

J. NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," September 2020

K. NIST SP 800-53A, Revision 5, "Assessing Security and Privacy Controls in Information Systems and Organizations," January 2022

L. NIST SP 800-60 Volume 1, Revision 1, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008

M. NIST SP 800-60 Volume II, Revision 1, "Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008

N. NIST SP 800-61, Revision 2, "Computer Security Incident Handling Guide," August 2012

O. NIST SP 800-63-3, "Digital Identity Guidelines," June 2017

P. NIST SP 800-84, "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities," September 2006

Q. NIST SP 800-88, Revision 1, "Guidelines for Media Sanitization," December 2014

R. NIST SP 800-92, "Guide to Computer Security Log Management," September 2006

S. NIST SP 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)," February 2007
T. NIST SP 800-95, "Guide to Secure Web Services," August 2007
U. NIST SP 800-100, "Information Security Handbook: A Guide for Managers," October 2006 (Updated March 2007)
V. NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment," September 2008
W. NIST SP 800-116, Revision 1, "Guidelines for the Use of PIV Credentials in Facility Access," June 2018
X. NIST SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," April 2010
Y. NIST SP 800-123, "Guide to General Server Security," July 2008
Z. NIST SP 800-124, Revision 2, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," March 2020
AA. NIST SP 800-128, "Guide for Security-Focused Configuration Management of Information Systems," August 2011 (Updated October 2019)
BB. NIST SP 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," September 2011
CC. NIST SP 800-160 Volume 2, Revision 1, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," December 2021
DD. NIST SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," April 2015
EE. NIST SP 800-161, Revision 1 "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," DRAFT October 28, 2021
FF. NIST SP 800-171, Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," February 2020 (Updated January 2021)
GG. NIST SP 800-181, Revision 1, "Workforce Framework for Cybersecurity Framework (NICE Framework)," November 2020
HH. NIST SP 800-184, "Guide for Cybersecurity Event Recovery," December 2016
II. NIST SP 800-192, "Verification and Test Methods for Access Control Policies/Models," June 2017
JJ. NIST SP 1800-11, "Data Integrity: Recovering from Ransomware and Other Destructive Events," September 2020
KK. NIST SP 1800-25, "Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events," December 2020
LL. NIST SP 1800-26, "Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events," December 2020

External Resources:

- NIAP Approved Products List
- NIST Cryptographic Module Validation Program
- NSA CSfC Components List
- NSA Media Destruction Guidance

[i] The Cybersecurity Framework (DHS CSF) Categories are groups of cybersecurity outcomes which can be linked to programmatic needs and associated with particular activities. Each Category contains Subcategories which make up the DHS Cybersecurity Framework.