DHS Risk Management Framework for Sensitive Systems

Attachment Y

Issue Date: August 1, 2022

This page intentionally left blank.

Table of Contents

I. Purpose

This Instruction implements the Federal Information Security Modernization Act of 2014 (FISMA) requirements to manage cybersecurity risk of Executive agency information technology and the Department of Homeland Security (DHS) Directive 140-01, Revision 2, Information Technology Security Program. This instruction further implements the National Institute of Science and Technology (NIST) Special Publication 800-37, Revision 2, "Risk Management Framework for Information Systems and Organization: A System Life Cycle Approach for Security and Privacy" and establishes the DHS Cybersecurity Risk Management Framework, processes and procedures applicable to all DHS Sensitive information technology (IT) systems (non-national security and intelligence systems).

Additionally, this Instruction outlines a cybersecurity risk management framework that can be used for implementing the NIST "*Framework for Improving Critical Infrastructure Cybersecurity*", also known as the "Cybersecurity Framework" or the "NIST Framework" as required by Executive Order 13800, "*Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*", May 11, 2017.

II. Scope

This Instruction applies to all DHS elements, employees, contractors, detailees, and others working on behalf of DHS, and users of DHS sensitive IT systems,

This Instruction shall not alter or supersede the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) or SCI within an SAP for intelligence as directed by Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended. Nor does it alter or supersede Department of Defense (DoD) authorities and policies as they apply to the United States Coast Guard.

This Instruction does not apply to National Security Systems (NSS). DHS Instruction: DHS National Security Systems: Risk Management, 4300B.101 provides the Cybersecurity Risk Management Framework for NSS.

III. Authorities

The following are primary authorities for the implementation of the DHS Cybersecurity Risk Management Framework for Sensitive Systems.

- Information Technology Management Reform Act, P.L. 104-106 (Clinger-Cohen Act of 1996)
- Federal Information Security Modernization Act of 2014 (FISMA), Public Law 113-283; 128 Stat 3073
- Executive Order 14028, "Improving the Nation's Cybersecurity", May 12, 2021
- Executive Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022
- OMB A-130, *Managing Information as a Strategic Resource*, 2016
- Executive Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, November 18, 2013

- OMB A-123, *Management's Responsibility for Internal Controls*, December 2004
-
- National Institute of Science and Technology (NIST) Federal Information Processing Standards and Special Publications.
- Cybersecurity & Infrastructure Security Agency (CISA) Binding Operational Directives
- DHS Directive MD 140-01, Rev 2, Information Technology Security Program
- DHS Delegation 04000, Delegation to the Chief Information Officer

IV. Roles and Responsibilities

This section lists personnel who have key roles in the RMF process and briefly describes the duties of each.

Authorizing Official (AO)

The AO formally assumes responsibility for operating an information system at an acceptable level of risk. The AO determines the degree of acceptable risk based on mission requirements, reviews the Security Authorization Package (SAP), and grants or denies an Authority To Operate (ATO). He or she shall be a senior management official and a Federal employee or member of the U.S. military.

The DHS CIO serves as the AO for all Department-level enterprise systems or designates an AO in writing. The Component CIO serves as the AO for Component information systems or designates one in writing. The DHS Chief Financial Officer (CFO) serves as the AO for CFO-designated systems managed at the DHS enterprise level. The Component CFO is the AO for only those CFO-designated systems managed by the Component.

Security Control Assessor (SCA)

The SCA should be a senior management official whose responsibilities include certifying the results of the security control assessment. The Component CISO assigns a SCA for their information systems in writing or to each information system. The SCA and the team conducting a certification must be impartial. They must be free from any perceived or actual conflicts of interest both with respect to the developmental, operational, and or management chains of command associated with the information system and with respect to the determination of security control effectiveness.

The SCA assesses the effectiveness of the security controls based on the documentation submitted in the security authorization package and makes a recommendation to the AO regarding whether to authorize the system. The SA team should coordinate closely with the SCA throughout the process to ensure they understand and meet DHS and Component requirements.

The SCA ensures that testing of security controls is documented in the security requirements traceability matrix (SRTM). The IACS application automatically creates the SRTM and the controls are tested to ensure that they have been implemented properly and are operating as intended. The security assessment is usually conducted using the security assessment plan developed by the SA team. To avoid conflict of interest members of the SA team should not be on the security assessment Team. This requirement need not apply for systems categorized as Low-Low-Low in the confidentiality, integrity, and availability security categories, providing an independent source validate test results for their completeness, consistency, and veracity.

The AO decides the required level of assessor independence based on:

- The criticality and sensitivity of the information system

- The ultimate risk to organizational operations, organizational assets, and individuals

- The level of assessor independence required for confidence that the assessment results are sound and valid for making credible risk-based decisions.

Figure V-1 illustrates the information hierarchy among various stakeholders needed to complete the Security Authorization process.

Compliance (or Risk Management) Team

The Compliance Team has primary responsibility for conducting security authorization activities. This includes collecting data, developing documents, and preparing the security authorization package for review by the SCA and AO. The Compliance Team may also conduct the security assessment depending on the need for separation of duties. The Compliance Team needs access to the DHS SA IACS tool. Figure V-2 shows the different stakeholders that must be engaged in order to conduct an efficient security authorization.

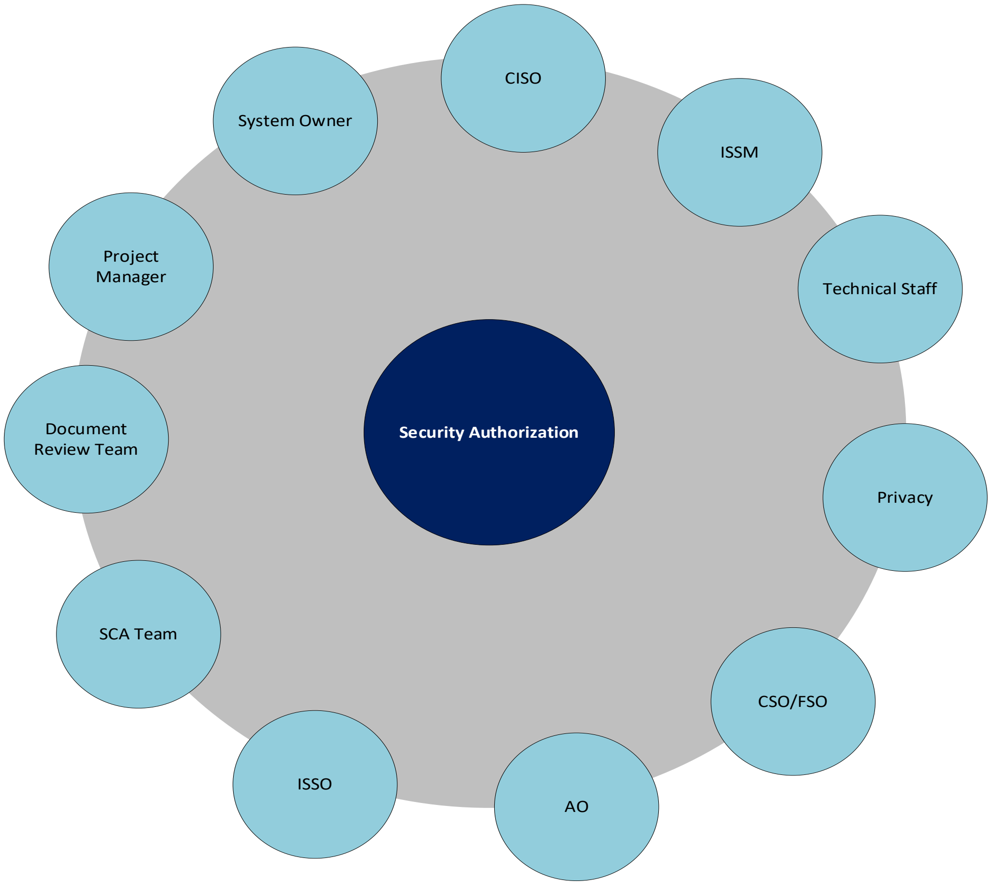


Figure 1: Security Authorization Team Stakeholders

Component CISO or Designee

The Components CISO or CISO delegated designee is responsible for ensuring security is addressed from inception, throughout the acquisition and system security engineering process before coordination and transition to the system's security team (i.e., ISSM, ISSO, etc.). CISO are responsible for:

- Overseeing the Component Cybersecurity Program and implementation of the Component's Cybersecurity Risk Management Framework in accordance with this DHS Instruction.
- Ensure that the Component CIO and DHS CISO are kept informed of all cybersecurity information system risks impacting the DHS enterprise or other Component information systems
- Maintain an independent Component-wide security control assessment program to ensure a consistent approach to controls effectiveness testing
- Ensure that an appropriate Security Operations Center (SOC) performs an independent network assessment as part of the security control assessment process for each authorized application
    - Implement and oversee a Plan of Action and Milestones (POA&M) program for remediation of indemnified vulnerabilities, findings, or weaknesses.

- Ensure that ISSOs are appointed for each information system

Information System Security Manager (ISSM)

ISSMs typically manage and oversee the cybersecurity of a collection of information systems or a major information system. Components should consider designating ISSMs as needed based on their operational needs. The Component CISO designates the ISSM in writing.

The ISSM plays a critical role in ensuring that the DHS cybersecurity program is implemented and maintained throughout the Component and is responsible for ensuring the following for information systems under their purview.

- Oversee the operational security of a Component information systems or collection of information systems.
- Ensure that the Component CISO is kept informed of all cybersecurity matters
- Ensure that all communications and publications pertaining to information security, including updates to the DHS policies are distributed to their assigned system(s) ISSOs and other appropriate stakeholders within their Component
- Validate all cybersecurity reporting for information systems
- Consult with the Component Privacy Officers or Privacy Points of Contact (PPOC) for reporting and handling of privacy incidents
- Manage information security including oversight and review of security requirements in procurement documents
- Ensure information systems periodically tested.
- Implement and manage a Plan of Action and Milestones (POA&M) processes for remediation through the creation of a POA&M for each known vulnerability

- Ensure cybersecurity incident reports are provided to the Component CISO
- Acknowledge receipt of Information Security Vulnerability Management (ISVM) messages, report compliance with requirements, or notify applicants of the granting of waivers
- Ensure adherence to the DHS specified Secure Baseline Configuration Guides
- Ensure training and oversight for personnel with significant responsibilities for cybersecurity
- Oversee the SA process for assigned systems
- Ensure that ISSOs monitor and manage the cybersecurity aspects of supply chain risks
- Ensure that ISSOs adopt software assurance principles and tools

Information System Security Officer (ISSO)

Information System Security Officers (ISSO) are not always directly responsible for conducting a security authorization, but they need to monitor and oversee the process at a minimum. ISSOs need to be aware of the status and expiration of the current ATO and initiate action early enough to ensure the security authorization process is completed before the system becomes operational or the current ATO expires. This entails working closely with the system owner or program manager to ensure that resources are available to both conduct and to participate in the security authorization process. Regardless of how the process is implemented, the ISSO plays a leading role to ensure documents are created and maintained in IACS and submitted to the SCA for validation. ISSOs should coordinate closely with the SCA and the AO before and during the security authorization process to ensure they are aware of requirements, processes, and expectations. For Components without ISSMs, the ISSO may also be responsible for the ISSMs duties. Component ISSOs are responsible for the following for information systems under their purview:

- Monitor security requirements for major application or general support system for compliance status.
- Ensure that requests for security authorization of information systems are completed in accordance with the published procedures
- Ensure compliance with all legal requirements concerning the use of commercial proprietary software, e.g., respecting copyrights and obtaining site licenses
- Maintain an inventory of hardware and software information systems
- Coordinate the development of a Contingency Plan and ensure that the plan is tested and maintained
- Ensure that risk assessments are completed to determine cost-effective and essential safeguards
- Ensure preparation of security plans for information systems
- Attend security awareness and related training programs and distribute security awareness information to the user community as appropriate
- Report IT security incidents (including computer viruses) in accordance with established procedures
- Report security incidents not involving IT resources to the appropriate security office
- Provide input to appropriate cybersecurity personnel for preparation of reports to higher authorities concerning sensitive and/or national security information systems

System Owner (or business owner)

The system owner must ensure that adequate resources are budgeted for and allocated to the security authorization process. The system owner will also serve as a primary source of input during data collection activities and should review the package for accuracy before it is forwarded to the SCA and AO. The system owner must also be involved in POA&M planning to help determine resource availability and schedule. System owners are ultimately responsible for the security of their systems and should be directly involved in the security authorization process.

Program Manager or Project Manager

The Program Manager may be a source of resources (e.g., if the security authorization process needs to be outsourced) and information input for areas where the system owner is not knowledgeable (e.g., contracts).

Technical Staff

A system's technical staff, including system administrators, database administrators (DBAs), and others, is the primary source of input for describing and implementing most technical controls identified in the security plan. They may also have input to the system categorization process depending on system technology (e.g., wireless) and configuration. The technical staff should provide input to the team creating the security assessment plan; the security assessment team will oversee the actual testing.

Chief Security Officer (CSO) and Facility Security Officer (FSO)

The Chief Security Officer (CSO) and the Facility Security Officer (FSO) are often responsible for the implementation of some controls (e.g., physical access controls) and may provide input needed for personnel and physical controls for the system.

Business Owner (combine with System owner)

The business owner may provide input needed for the system categorization and section one (1) of the security plan. The business owner may also provide resources for conducting the security authorization or remediating weaknesses.

Privacy Officer

The DHS Chief Privacy Officer (CPO) is responsible for the implementation of NIST SP 800-53R5 Appendix J. The CPO will consult with other agency officials, including Program Managers, Information System Owners, AOs, CIOs, and CISOs in fulfilling this responsibility. The authority, however, for selection and assessment of privacy controls ultimately rests with the CPO.

The DHS CPO reviews all Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Records Notices (SORN), providing approval as appropriate. The Privacy Office also selects and implements the privacy controls for each system. ISSOs and System Owners are not part of this process and must not modify the privacy controls.

DHS Document Review Team (DR)

The DHS Document Review (DR) Team reviews and validates security authorization packages once they are completed in IACS.

POA&M Manager

- Serves as the primary point of contact for Component POA&M and Waiver management
- Serves as a liaison to DHS OCISO on any matters related to POA&Ms and Waivers.
- Responsible for holding the POA&M Risk Board Meetings with all the stakeholders (IT PM, System Owner, ISSO, System Admins, Development Team)

- Reviews Waivers prior to sending to DHS OCISO for approval
- Ensures approved active Waivered POA&Ms do not show up as a failed POA&M on the FISMA Scorecard
- Reviews Waiver expirations quarterly and ensures expired waivers are removed from IACS and POA&Ms are updated accordingly.
- Ensures POA&M Quality issues are disseminated to the ISSOs/ISSMs weekly and resolved
- Ensures System and Program POA&M's are managed properly and disseminated to the Program Managers and stakeholders for resolution
- Ensures CFO Designated System POA&Ms and Audit (A-123, Financial, GAO, ITAR, OIG, etc.) related POA&Ms are created, reported, and mitigated in a timely manner
- Reviews and approves the POA&M Cancellation requests for the Component
- Updates POA&M status in IACS for Cancellations and Waivers
- Ensures annual training is provided to ISSOs/ISSMs and other stakeholders on POA&Ms and Waivers
- Monitors POA&M progress from creation to remediation.
- Provides POA&M and Waiver status reports to Component Management

OA Manager

- Manages the Component OA Program
- Provides recommendations to the CISO and AO on triggers, subsequent impacts, and systems entering the OA Program
- Defines and updates the Organization defined frequencies for security controls reviews for the Component
- Submits the OA Report(s) to the CISO and AO to document risk status of all systems participating in the OA program.
- Provides guidance to ISSOs regarding the OA Process
- Provides OA Training to ISSOs and System stakeholders on the Component OA Process on a regular basis
- Prepares recommendations to the CISO and AO based on ORMB feedback
- Creates and submits OA Recommendation Letter to the CISO and AO for their review and revisions

- Facilitates OA meetings with the OA Risk Management Board (ORMB)
- Collects all input from the ORMB
- Adjudicating escalated system triggers
- Facilitating system Risk Elements in IACS
- Monitoring and evaluating reported trigger events against established risk thresholds
- Engaging the appropriate stakeholders based on specific triggers and systems

V. RMF Processes and Procedures

The Federal Information Security Modernization Act of 2014 (FISMA) requires all Federal departments and agencies to establish a Cybersecurity Program to protect government information, operations, and assets against natural or man-made threats. NIST Special Publication (SP) 800-37R2, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach" specifies the required risk management framework.

NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View statues that managing risk is a complex, multifaceted activity that requires the involvement of the entire organization—from senior leaders/executives providing the strategic vision and top-level goals and objectives for the organization; to mid-level leaders planning, executing, and managing projects; to individuals on the front lines operating the information systems supporting the organization's missions/business functions. Risk management is a comprehensive process that requires organizations to: (i) *frame* risk (i.e., establish the context for risk-based decisions); (ii) *assess* risk; (iii) *respond* to risk once determined; and (iv) *monitor* risk on an ongoing basis. Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization. The complex relationships among missions, mission/business processes, and the information systems supporting those missions/processes require an integrated, organization-wide view for managing risk.

Integration with Enterprise Risk Management and Internal Control

Some risks are so large or cross cutting that they are significant to the organization and therefore, require the involvement and oversight of the highest level of leadership and management. Enterprise Risk Management (ERM) evolved out of the growing awareness that risks must be managed holistically with the total organization in mind. It seeks to integrate risk management practices into an enterprise-wide, standardized approach, and incorporate risk awareness into strategic and decision-making.

Components shall establish and maintain cybersecurity risk management programs that integrate with their ERM program to identify and manage risks that potentially impact the achievement of their organization's mission. This includes elevating risks that require the attention of Department senior leadership based on pre-established departmental risk tolerance thresholds

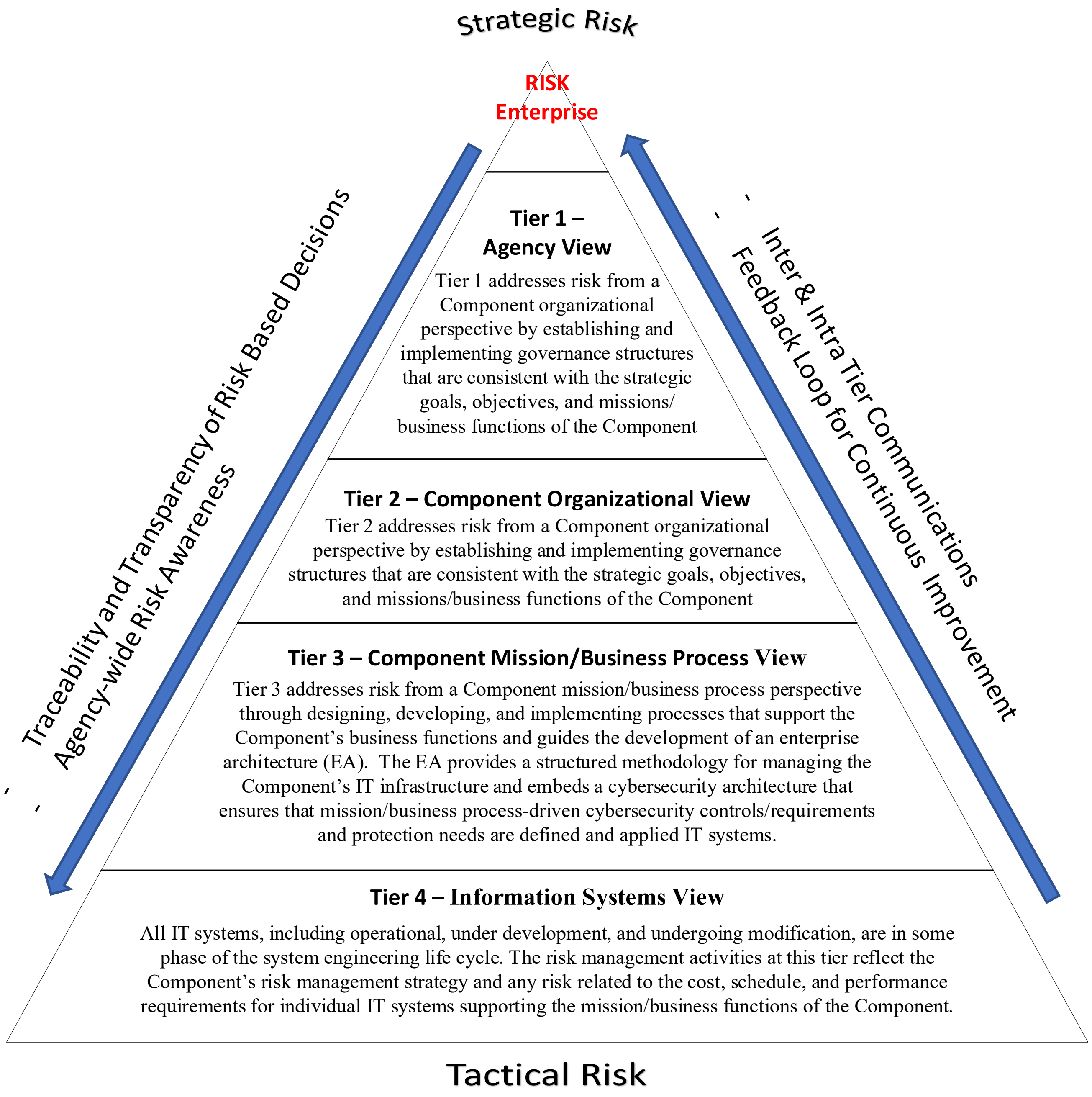
The calculated cybersecurity risk carried by each Component system is a subset of the Component's overall operational (mission and organization) risk Component system, mission, and organizational risks are a subset of overall Departmental cybersecurity and enterprise risk.

The DHS cybersecurity strategy integrates risk management throughout the Department using a four-tiered approach. The approach addresses risk at the Agency level, Component organization level, mission/business process level, and IT system level.

- **TIER ONE: AGENCY VIEW (Agency Governance)** Tier 1 addresses risk from a DHS organizational perspective by establishing and implementing governance structures that are consistent with the strategic goals, objectives, and missions/business functions of DHS and the requirements defined by federal laws, regulations, directives, and other authorities. policies, standards, and. guidance. Governance structures provide oversight for the risk management activities conducted by Component and include: (i) the establishment and implementation of a DHS cybersecurity risk executive (function); (ii) the establishment of the DHS risk management strategy including the determination of risk tolerance; and (iii) the development and execution of DHS-wide investment strategies for information resources and information security.
- **TIER TWO—COMPONENT ORGANIZATIONAL VIEW (Component Governance)** Tier 2 addresses risk from a Component organizational perspective by establishing and implementing governance structures that are consistent with the strategic goals, objectives, and missions/business functions of the Component and the requirements defined by federal laws, regulations, directives, DHS Governance structures - policies, standards, and guidance. Governance structures provide oversight for the risk management activities conducted within the Component and include: (i) the establishment and implementation of a risk executive (function); (ii) the establishment of the Component's risk management strategy including the determination of risk tolerance; and (iii) the development and execution of Component-wide investment strategies for information resources and information security.
- **TIER THREE—COMPONENT MISSION/BUSINESS PROCESS VIEW Mission/Business Processes (Information and Information Flows)** Tier 3 addresses risk from a Component mission/business process perspective by designing, developing, and implementing mission/business processes that support the Component organization functions defined at Tier 2. Component mission/business processes guide and inform the development of an enterprise architecture that provides a disciplined and structured methodology for managing the complexity of the Component's information technology infrastructure. A key component of the enterprise architecture is the embedded information security architecture that provides a roadmap to ensure that mission/business process-driven information security requirements and protection needs are defined and allocated to appropriate organizational IT systems and the environments in which those systems operate.
- **TIER FOUR—INFORMATION SYSTEMS VIEW (Environment of Operation)** All IT systems, including operational, under development, and undergoing modification, are in some phase of the system engineering life cycle. In addition to the risk management activities carried out at Tier 1-3, risk management activities are also integrated into the system development life cycle of organizational IT systems. The risk management activities at this tier reflect the Component's risk management strategy and any risk related to the cost, schedule, and performance requirements for individual IT systems supporting the mission/business functions of the Component. Risk

management activities take place at every phase in the system development life cycle with the outputs at each phase influencing subsequent phases.

All levels of the risk management hierarchy have information that is relevant and useful to the other tiers and therefore have a responsibility to provide such information. To be effective, the flow of information between leadership, managers, and practitioners, needs to be flexible enough to accommodate multi-directional communications, not just top down from senior officials to staff and not just at the system level. The RMF must complement and support DHS's acquisition management system activities, milestones, and phases, as reflected in DHS Instruction 102-01-001, Revision 1, 3 May 2019. The integration DHS cybersecurity methodology is depicted in Figure VI-1, DHS Sensitive Systems Cybersecurity Risk Management Integration.


Strategic Risk
RISK
Enterprise
Traceability and Transparency of Risk Based Decisions
Agency-wide Risk Awareness
Inter & Intra Tier Communications
Feedback Loop for Continuous Improvement
Tactical Risk

Tier 1 – Agency View

Tier 1 addresses risk from a Component organizational perspective by establishing and implementing governance structures that are consistent with the strategic goals, objectives, and missions/ business functions of the Component

Tier 2 – Component Organizational View

Tier 2 addresses risk from a Component organizational perspective by establishing and implementing governance structures that are consistent with the strategic goals, objectives, and missions/business functions of the Component

Tier 3 – Component Mission/Business Process View

Tier 3 addresses risk from a Component mission/business process perspective through designing, developing, and implementing processes that support the Component's business functions and guides the development of an enterprise architecture (EA). The EA provides a structured methodology for managing the Component's IT infrastructure and embeds a cybersecurity architecture that ensures that mission/business process-driven cybersecurity controls/requirements and protection needs are defined and applied IT systems.

Tier 4 – Information Systems View

All IT systems, including operational, under development, and undergoing modification, are in some phase of the system engineering life cycle. The risk management activities at this tier reflect the Component's risk management strategy and any risk related to the cost, schedule, and performance requirements for individual IT systems supporting the mission/business functions of the Component.

Figure VI-1, DHS Cybersecurity Risk Management Integration.

The system owner and program manager are responsible for ensuring risk is addressed as early as possible during the Acquisition Lifecycle Framework (ALF) and the RMF, and that adequate security is incorporated to sufficiently mitigate identified risk. The. RMF activities must be initiated as early as possible in the DHS acquisition process and fully coordinated and specific requirements for integrating cybersecurity through the Acquisition Lifecycle is further denoted in DHS Instruction 102-01-012, Cybersecurity through the Acquisition Lifecycle Framework.

..

The DHS CISO working with the Component CISO reviews program risk, threat analysis, and recommendations provided by the component. This review helps all components determine the level of aggregate risk to systems and appropriate mitigation of identified risks to information systems. These risk reviews are used to inform Acquisition Review Board decisions throughout the ALF, as required by MGMT 102-001 and explained in the 102-01-012 Instruction.

Component AOs approve a system to operate within the authorization boundaries as determined by the component enterprise. The risk determination and acceptance of an approved system affects the risk of all the other interfaced systems operating within the component enterprise, and may impact the mission of the component. Accepted risk at the component enterprise level in turn affects the risk level and mission of other components and the DHS enterprise overall.

Threat Environment

One major aspect of cybersecurity risk management strategy is the identification of the DHS threat environment. A **cybersecurity threat** is any circumstance or event with the potential to adversely impact DHS operations (including mission, functions, image, or reputation), DHS assets, individuals, other organizations, or the Nation through, and DHS information and information systems intended to compromise the security of the information system by altering the availability, integrity, or confidentiality of a system or the information it contains. DHS has identified the high-level threats to the Department and the associated threat actors in the proceeding sections.

Cybersecurity Threats

- **Technical Exploitation:** Technical threats attempt to exploit vulnerabilities, weaknesses, or flaws in the design, implementation, operation, or management of an information system, device, or service that provides access to cybersecurity threat actors. Malicious code and flaws in software coding or system configuration are common technical threats.

- **Human Exploitation**: Human threats are methods that target human vulnerabilities or weaknesses such as carelessness and trust. Social engineering threats are the most common threats in this category. Threat actors use social engineering to trick an individual into inadvertently allowing access to a system, network, or device. Phishing and spear-phishing are common **social engineering** techniques.

- **Natural Disasters or Events:** Natural threats are events in nature that can occur and cause damage to information systems and capabilities but that threat actors can also exploit for their use because of a break down in cybersecurity controls. Every location comes with some potential for a natural emergency or an event to occur. Hurricanes, tornados, floods, fires, and earthquakes can periodically occur. Each region and specific DHS location has common but also specific natural threats. The natural threats specific to a region or location must be determined and considered as part of risk management activities.

Cybersecurity Threat Actors

Cybersecurity threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities/weaknesses, low cyber security awareness, and technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks. The globalized nature of the Internet allows these threat actors to be physically located anywhere in the world and still affect the security of DHS information systems. DHS has identified the actors as posing a threat to the Department.

- **Nation-states** are frequently the most sophisticated threat actors, with dedicated resources and personnel, and extensive planning and coordination.
- **Cybercriminals** are generally understood to have moderate sophistication in comparison to nation-states. Nonetheless, they still have planning and support functions in addition to specialized technical capabilities that affect many victims.

Threat actors in the top tier of sophistication and skill, capable of using advanced techniques to conduct complex and protracted campaigns in the pursuit of their strategic goals, are often called **advanced persistent threats (APT)**. This designator is usually reserved for nation-states or very proficient organized crime groups.

- **Hacktivists, terrorist groups**, and **thrill-seekers** are typically at the lowest level of sophistication as they often rely on widely available tools that require little technical skill to deploy. Their actions often have no lasting effect on their targets beyond reputation.
- **Insiders** are individuals working within their organization who are particularly dangerous because of their access to internal networks that are protected by security perimeters. Access is a key component for malicious threat actors and having privileged access eliminates the need to employ other remote means. Insider threats may be associated with any of the other listed types of threat actors but can also include disgruntled employees with motive.

DHS Cybersecurity Risk Management Framework:

DHS has established and implemented the DHS Cybersecurity Risk Management Framework to meet the requirements specified in complying with the requirements of OMB A-130 and FISMA.

Risk Management Compliance Tools:

DHS has implemented an Information Assurance Compliance System (IACS) to automate processes of the RMF. The tool facilitates the Framework activities and steps to track, monitor, and report on the overall compliance and DHS cybersecurity risk posture. Sensitive systems are tracked and recorded in the IACS application.

Applying the Risk Management Framework to DHS Sensitive Information Technology Systems and Information

The Cybersecurity Framework enables organizations to apply the principles and best practices of risk management to improve security and resilience. The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references. The Core presents industry standards, guidelines, and best practices, in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous functions:

Identify – Develop an organization understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect – Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.

Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

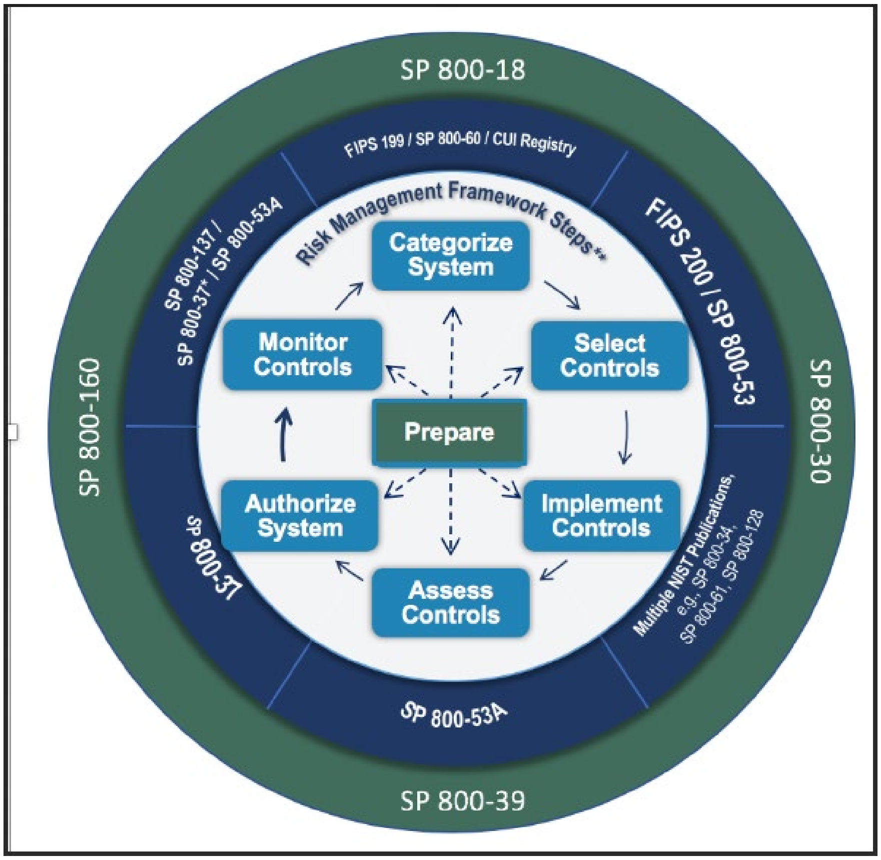
Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Risk Management Framework Phases

The RMF provides a disciplined and structured process that integrates information security and risk management activities with ALF and the SELC.

The DHS RMF consists of a seven-phase process that emulates the NIST RMF methodology documented in the NIST Special Publication 800-37R2, Risk Management Framework for Information Systems and Organizations-A System Life Cycle Approach for Security and Privacy. This process parallels the ALF and the system engineering life cycle (SELC), with the RMF activities being initiated at program or system inception (e.g., documented during capabilities identification or at the implementation of a major system modification). The DHS risk management framework is depicted in Figure VI-2, DHS Cybersecurity RMF.



VI-2: DHS Cybersecurity RMF

Each DHS RMF phases contain several sub activities that should be completed within that step prior to moving to subsequent steps. Although the phases activities are described below sequentially, DHS Components may need to execute certain activities in an iterative manner or in different phases of the system engineering life cycle. NIST has published supporting Federal Information Processing Standards (FIPS) or Special Publications (SP) to provide direction and clarifying procedure to facilitate the completion of each phase.

RMF Workflow Activities Descriptions.

There are seven steps in the RMF; a preparatory step to ensure that organizations are ready to execute the process and six main steps. All seven steps are essential for the successful execution of the RMF. The steps are:

- Prepare to execute the RMF from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk.

- Categorize the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.26

- Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.

- Implement the controls and describe how the controls are employed within the system and its environment of operation.
- Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
- Authorize the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
- Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

The seven phases of the RMF and the organizational activities required to prepare for the RMF implementation are depicted in Table: *Table VI-2:*

Phase 0, Prepare
TASK P-1: RISK MANAGEMENT ROLES • Individuals are identified and assigned key roles for executing the Risk Management Framework. TASK P-2: RISK MANAGEMENT STRATEGY • A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. TASK P-3 RISK ASSESSMENT—ORGANIZATION • An organization-wide risk assessment is completed, or an existing risk assessment is updated. TASK P-4: ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (OPTIONAL) • Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles are established and made available. TASK P-5: COMMON CONTROL IDENTIFICATION • Common controls that are available for inheritance by organizational systems are identified, documented, and published. TASK P-6: IMPACT-LEVEL PRIORITIZATION (OPTIONAL) • A prioritization of organizational systems with the same impact level is conducted. TASK P-7: CONTINUOUS MONITORING STRATEGY—ORGANIZATION • An organization-wide strategy for monitoring control effectiveness is developed and implemented.
Phase 1: Categorize

TASK C-1: SYSTEM DESCRIPTION

- The characteristics of the system are described and documented.

TASK C-2: SECURITY CATEGORIZATION

- A security categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed.
- Security categorization results are documented in the security, privacy, and SCRM plans.
- Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes.
- Security categorization results reflect the organization's risk management strategy.

TASK C-3: SECURITY CATEGORIZATION REVIEW AND APPROVAL

- The security categorization results are reviewed, and the categorization decision is approved by senior leaders in the organization.

Phase 2: Select Controls

TASK S-1: CONTROL SELECTION

- Control baselines necessary to protect the system commensurate with risk are selected.

TASK S-2: CONTROL TAILORING

- Controls are tailored producing tailored control baselines.

TASK S-3: CONTROL ALLOCATION

- Controls are designated as system-specific, hybrid, or common controls.
- Controls are allocated to the specific system elements (i.e., machine, physical, or human elements).

TASK S-4: DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS

- Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents.

TASK S-5: CONTINUOUS MONITORING STRATEGY—SYSTEM

- A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed.

TASK S-6: PLAN REVIEW AND APPROVAL

- Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official.

Phase 3: Implement Controls

TASK I-1: CONTROL IMPLEMENTATION

- Controls specified in the security and privacy plans are implemented.
- Systems security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans.

TASK I-2: UPDATE CONTROL IMPLEMENTATION INFORMATION

- Changes to the planned implementation of controls are documented.
- The security and privacy plans are updated based on information obtained during the implementation of the controls.

Phase 4: Assess Controls

TASK A-1: ASSESSOR SELECTION

- An assessor or assessment team is selected to conduct the control assessments.
- The appropriate level of independence is achieved for the assessor or assessment team selected.

TASK A-2: ASSESSMENT PLAN

- Documentation needed to conduct the assessments is provided to the assessor or assessment team.
- Security and privacy assessment plans are developed and documented.
- Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required.

TASK A-3: CONTROL ASSESSMENTS

- Control assessments are conducted in accordance with the security and privacy assessment plans.
- Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered.
- Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments.

TASK A-4: ASSESSMENT REPORTS

- Security and privacy assessment reports that provide findings and recommendations are completed.

TASK A-5: REMEDIATION ACTIONS

- Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken.
- Security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions.

TASK A-6: PLAN OF ACTION AND MILESTONES

- A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed.

Phase 5: Authorize the System

TASK R-1: AUTHORIZATION PACKAGE

- An authorization package is developed for submission to the authorizing official.

TASK R-2: RISK ANALYSIS AND DETERMINATION

- A risk determination by the authorizing official that reflects the risk management strategy including risk tolerance, is rendered.

TASK R-3: RISK RESPONSE

- Risk responses for determined risks are provided.

TASK R-4: AUTHORIZATION DECISION

• The authorization for the system or the common controls is approved or denied. TASK R-5: AUTHORIZATION REPORTING • Authorization decisions, significant vulnerabilities,
Phase 6: Monitor
TASK M-1: SYSTEM AND ENVIRONMENT CHANGES • The information system and environment of operation are monitored in accordance with the continuous monitoring strategy. TASK M-2: ONGOING ASSESSMENTS • Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy. TASK M-3: ONGOING RISK RESPONSE • The output of continuous monitoring activities is analyzed and responded to appropriately. TASK M-4: AUTHORIZATION PACKAGE UPDATES • Risk management documents are updated based on continuous monitoring activities. TASK M-5: SECURITY AND PRIVACY REPORTING A process is in place to report the security and privacy posture to the authorizing official and other senior leaders and executives. TASK M-6: ONGOING AUTHORIZATION • Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions. TASK M-7: SYSTEM DISPOSAL • A system disposal

Table VI-2: RMF Workflow Activities Descriptions

Organization Cybersecurity Risk Management Preparation

Prior to implementing the RMF for a specific IT system, the organization must determine and understand organizational risk as related to core missions and business functions. This initial preparation sets the foundation for overall cybersecurity risk management that specific IT system risk are further built upon. Specific activities and further detailed in the 102-01-012.

Identify Organizational Personnel and Responsibilities

The RMF organizational personnel are the senior leaders who have responsibilities for assuring the organization effectively meets its core mission goals. They include the most senior organization executive, CFO, CIO, CSO, and CISO. Components need to ensure that their organizational personnel understand their RMF roles and responsibilities and are appropriately trained on their roles and the DHS RMF.

Organizational and Mission Risk Assessment (RA)

Managing risk is a complex, multifaceted activity that requires the involvement of the entire organization—from senior leaders/executives providing the strategic vision and top-level goals and objectives for the organization; to mid-level leaders planning, executing, and managing projects to individuals on the front lines operating the information systems supporting the organization's missions/business functions. Risk Management requires:

(1) Framing risk
(2) Assessing risk
(3) Responding to risk once it has been determined
(4) Monitoring risk on an ongoing basis.

As part of this risk management process, there are risk functions that are broken out on different levels which intertwine to form a comprehensive risk strategy as described at the beginning of this section.

Agency risk provides the context (frame) for which everything else is assessed. This is provided in DHS policy 140-01.01, DHS Cybersecurity Program Policy for Sensitive and National Security Systems and agency level lines-of business continuity and devolution plans. This provides prioritization of missions and business functions at the DHS agency level which in turn drives investment strategies and funding decisions, thus, affecting the development of enterprise architecture (including embedded information security architecture).

Organizational risk provides the context (frame) for which Components specific mission and business functions are assessed. This should be specified and provided in Component specific policy, business continuity and recovery plans and continuity of operation plans. Together, this provides a prioritization of missions and business functions which in turn drives investment strategies and funding decisions at the Component level, thus, affecting the development of enterprise architecture (including embedded information security architecture) and the allocations and deployment of management, operational, and technical security controls at the system level.

To determine a Components organizational level risk, the Component should conduct a high-level risk assessment (RA) considering Component specific missions, exposure, threats, threats agents, and business functions. The RA results are used to establish a Components specific cybersecurity risk strategy, risk tolerance, and plans for managing Component level organizational cybersecurity risk which is then used to managing risk at the IT system level as described in the following sections.

Project and System Personnel

The project personnel are the people who have responsibilities for assessing the information system. For example, they include the AO, ISSM, ISSO, System Owner, and Program or Project Manager. This information is usually known in advance of the IT system technical design. Components need to ensure that their project and system personnel understand their RMF roles and responsibilities and are appropriately trained on their roles and the DHS RMF.

System Boundary

FISMA requires DHS to create, implement, and maintain an official inventory of major information systems operated by or under the control of DHS. A major information system is defined in OMB Circular A-130 as "a system that is part of an investment that requires special management attention as defined by OMB guidance and agency policies, a 'major automated information system' as defined in 10 U.S.C. § 2445, or a system that is part of a major acquisition as defined in OMB Circular A-11, *Capital Programming Guide*, consisting of information resources." Major information systems are categorized as either General Support Systems (GSS) or Major Applications (MA).

One major aspect of categorization to determine if an IT system is a GSS or MA and specific to the IT system is uniquely assigning and identifying the information resources of IT system which defines the system boundary. This can be accomplished early in the system planning based on the initial business case and planned system concept. The system boundary as planned should generally be under the same direct management and funding control so support the specific business base. Direct management control does not necessarily imply that there is no intervening management. The actual boundary is defined by the Components and should include the project and system personnel. The IT system must also be categorized as either a GSS or a MA.

A GSS is an interconnected set of information resources under the same direct management control which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. It can be, for example, a Local Area Network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information resource between organizations.

An MA is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Certain applications require special management oversight and security and should be treated as MAs because of the nature of the information stored in or processed by them.

As the IT system progresses through the RMF phases and the SELC phases, all hardware, software, and firmware are documented as part of the system boundary. A high-level definition of technologies may be described and subsequently defined as the system is developed. For example, the system may require a database but the specific database application (Oracle, SQL Server, etc.) may not be determined until later. Hardware, software, and firmware tend to be interrelated and this should also be documented in the implementation of security controls.

For more information on determining boundaries, please see the DHS FISMA Inventory Methodology available at: http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/ComplianceDocs.aspx

Develop the Security Plan

Once the system boundary is determined, the next activity is to describe and document the system in a security plan. A security plan is a formal document which provides an overview of the security requirements for an IT system or an information security program and describes the security controls in place or planned for meeting those requirements. It is a living document requiring periodic review, modification. As the IT system progresses through the RMF phases additional information should be updated into the security plan leading to a completed document for use in the Authorization to Operate phase. The initial SP should be created documenting the information known from the planning stages. This includes project and system personnel, a summarized description of the system, the system boundary, etc. The SP must be created and development in DHS IACS.

In later phases of the SELC and RMF, all equipment (hardware), software, ports and protocols in use, and interconnections associated with the IT system will be identified and inventoried in the security plan. Each piece of equipment should be characterized in as much detail as possible, including description, network address, operating system, firmware, etc... Software is a collection of computer instructions which allows the creation, transmission, and storage of data in an information system as well as its essential operation. It includes operating systems, computer programs (applications), software libraries, and databases. All software should be accounted for and inventoried in the SP.

Configuration Management

Another key activity that should be established early in the SELC and the RMF is the creation of capabilities to manage the system design, requirements implementation, documentation, and track and approve changes through the phases. Employing strong configuration management and control processes helps to ensure that system functional and security requirements are appropriately implemented in the system, documentation is maintained and available when needed, and changes are appropriately managed. A configuration management board should be established to appropriately track and management the system through the SELC and the RMF.

Phase 0 and Phase 1: Security Categorization

Security categorization is the process of determining the potential security impact level of the system. The purpose of this activity is to determine the adverse impact or consequences to the organization with respect to the confidentiality, integrity, and availability of the system and the information processed, stored, and transmitted. The mission and business functions are used to select system data types. Common program or system data types are identified in the NIST SP 800-60, Vol. 2 Revision. 1, Guide for Mapping Types of Information, and Information Systems to Security Categories: Appendices and are available for selectin in the IACS. The NIST FIPS 199 security categorization process is used to determine a final impact level for each of the three security objectives: confidentiality, integrity, and availability.

System data types can be mapped DHS BRM lines of business and mission which the information system supports. Each system data type has a predetermined impact for each security objective. This impact may be adjusted based on a risk assessment, risk elements, and other types of information that may require increased security.

Categorization of the system is a coordinated effort between the Program Manager (PM), ISSM, ISSO, System Owner, Data Owner, and Privacy point of contact.

CFO-designated Systems

This section explains the distinctions to be used for proper classification of CFO-designated systems, financial systems, and mixed financial systems. CFO-designated Systems are those that store, process, or transmit financial data that is material to (i.e., can have a significant impact on) the DHS financial statement and therefore require additional management accountability and effective internal control. These systems can include financial systems as well as non-financial systems and significantly support financial processes.

Financial systems include those that have a primary function to store or process financial data. This includes any system which is used for any of the following:

- Collecting, processing, maintaining, transmitting, and reporting data about financial events
- Supporting financial planning or budgeting activities
- Accumulating and reporting cost information
- Supporting the preparation of financial statements

Mixed financial systems are those that support both financial and non-financial functions. Mixed financial systems may or may not be on the CFO-designated list.

All CFO-designated Systems must be assigned a minimum impact level of "moderate" for confidentiality, integrity, and availability. If warranted by risk-based assessment, the integrity objective should be elevated to "high."

Privacy Systems

This section explains the distinctions to be used for proper classification of system containing PII or SPII. The DHS Chief Privacy Officer establishes guidance on DHS privacy policy and oversees all compliance activities of privacy controls, as it relates to NIST SP 800-53R5 Appendix J, "*Privacy Control Catalog*". The DHS Chief Privacy Officer is a key stakeholder in this process. For Privacy compliance activities, follow the guidance from DHS Directive 047-01.

The CPO designates Privacy Sensitive Systems based on adjudicated Privacy Threshold Analyses (PTA), which are conducted for all systems. Privacy Sensitive Systems are those that maintain Personally Identifiable Information (PII) about either DHS personnel or members of the public.

Privacy Sensitive Systems should meet the following requirements:

- Privacy systems must be at least a **"moderate"** for confidentiality, per the *DHS 4300A Sensitive Systems Handbook*.
- As part of the Security Authorization Process, PTAs are sent to the Component Privacy office via Component-specific procedures. PTAs are subsequently sent to, reviewed, and approved by the DHS Privacy Office. The Privacy Office decides whether a system is a Privacy Sensitive System and whether additional privacy compliance documentation, such as a Privacy Impact Assessment (PIA) or System of Records Notice (SORN), is required. Inquiries regarding the status of a PTA should be directed to a program's Component Privacy office.
- The CPO is responsible for oversight of all privacy incident management and must be informed expeditiously of all incidents involving Privacy Sensitive Systems.
- Assessment of privacy controls has to be conducted by the DHS Privacy Office, but all inquiries should be directed to the Component Privacy office.

Records Schedule

All Federal records, regardless of format, must be scheduled (44 U.S.C. 3303) either by an agency schedule or a General Records Schedule (GRS) approved by National Archives and Records Administration (NARA).

A records schedule is a comprehensive list and description of records grouped together based on function or subject. The schedule provides mandatory instructions for the disposition of the records (including the transfer of permanent records and disposal of temporary records) when they are no longer needed by the agency. As part of the ongoing records life cycle, disposition should occur in the normal course of agency business. Records that do not fall under a NARA approved records schedule cannot be legally destroyed. Unscheduled records are considered permanent until a records schedule is approved by NARA.

Agencies are required by law to develop records schedules for all of their records not covered by the GRS (44 U.S.C. 3303). After reviewing their records, agencies submit the schedules for NARA approval. The schedule contains descriptions of record series and disposition instructions for each record. These instructions specify when the series is to be cut off, when eligible temporary records must be destroyed, and when permanent records are to be transferred to the National Archives. Schedules may not be implemented until NARA has approved them. Some schedules, especially those containing records relating to financial management, claims, and other related matters, must also be approved by the General Accounting Office (GAO) (44 U.S.C. 3309) before NARA will approve them. Once approved by NARA, retention periods in the schedules are mandatory and authorize the systematic removal of unneeded records from Federal offices.

These two URLs will link to the National Archives and Records Administration.

DHS Schedules : This page contains all the schedules submitted to NARA for approval. As the custodian for the schedules, NARA is responsible for these records.

GRS Schedules: Transmittal 29 represents the latest update to the GRS and includes all recent revisions and supersessions.

Continued Assessment of Risk

Once the security categorization is completed the initial risk assessment should be updated reviewed to ensure the results of security categorization are consistent with the organization’s risk management strategy. Risk assessments are conducted throughout the RMF as information is determined and the system progresses through the SELC. Risk assessments are an important activity for evaluating risk of a system in context of mission/business activities and functions it supports.

Information determined during this activity must be captured in the SP and the initial risk assessment report, as appropriate, and maintained and updated throughout the RMF to reflect the most recent information.

Once the security categorization is completed, the categorization is identified in DHS IACS.

Register the System

Upon completion of the system security categorization, the system must be registered for accountability and security oversight, by using the FISMA ID. FISMA requires that all major systems be accounted for and annually reported on in the annual agency FISMA report to OMB. Components must register their major applications with the DHS FISMA Inventory Management Team.

E-Authentication

Electronic Authentication (eAuth) is the process of establishing confidence in user identities that are presented in online environments. For local or remote authentication, application developers are often faced with a choice of mechanisms based on a wide variety of technologies. The use of Multifactor Authentication (MFA) adds an increased layer of security to transactions by using multiple forms of eAuth mechanisms during a transaction.

OMB requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. OMB Memorandum 04-04 Attachment A establishes and describes four levels of identity assurance for electronic transactions requiring authentication. Assurance levels also provide a basis for assessing Credential Service Providers on behalf of Federal agencies.

Prepare and Submit a Privacy Threshold Analysis

All DHS Privacy Office must review all major systems to determine whether it is privacy sensitive and whether additional privacy compliance documentation will be required. The Component must complete a Privacy Threshold Analysis (PTA), Privacy Impact Analysis (PIA), and the System of Record Notice (SORN) and submit the completed analysis to the DHS Privacy Office.

More information is available at: PTA Template Guidance

Once the DHS Privacy Office reviews the PTA, the PIA, and the SORN, the associated documentation is uploaded to IACS.

Phase 2: Select Security Controls

Once the security categorization is completed the DHS baseline security controls are used to select the controls applicable to the system. The DHS controls contain both NIST security controls specific in the SP 800-53R5, Security and Privacy Controls for Federal Information Systems and Organizations and DHS specific derived controls. Although this baseline provides a minimum set of controls, the Component, AO, system owner, and ISSO may determine that additional or more stringent controls are necessary to mitigate risk to an acceptable level. Other considerations should also be considered when selecting controls. For example, DHS CFO-designated systems have specific controls that must be evaluated, tested, and documented annually to reduce the overall risk to an acceptable level.

Security controls are selected based on the system categorization, the mission of the organization, the relationship of the IT system to other systems (e.g., common controls, interconnection security agreements, Memorandums of Agreement (MOA) and Memorandums of Understanding (MOU), and technology considerations such as wireless and Bluetooth, and cost- benefit analyses). During the security control selection process organizations may begin planning for the continuous monitoring process by developing a monitoring strategy. The strategy can include, for example, monitoring criteria such as the volatility of specific security controls and the appropriate frequency of monitoring specific controls. Typically, the component will have a continuous monitoring program to provide overall guidance, requirements, and monitoring of certain controls. The system owner and ISSO can leverage and supplement this component program with a strategy that is tailored to the system to provide coverage to any area the component continuous monitoring program may not be able to cover.

Selection of the security controls is accomplished in DHS IACS. Once the security controls are selected the controls are documented in the in a system security plan (SSP). The DHS IACS tool facilitates this activity automatically selecting the associated security controls for the system based on the entered security categorization information.

NIST 800-53R5 security controls as published contain sections for embedded parameters to be specified by the organization. The DHS baseline controls contain the DHS expected parameter for the controls and are automatically populated from the IACS.

Privacy controls are under the authority of and determined by the Privacy Office. ISSOs and system owners are not to address these controls.

In some cases, a topical overlay of security controls may be required. An overlay is a specification of security controls, control enhancements, supplemental guidance, and other supporting information considered during the tailoring process, with the purpose of complementing or further defining established security control baselines. Overlays may be more stringent or less stringent than the initial security control baseline and therefore can result in the addition or subtraction of controls.

Applying one or more required overlays provides a structured form of tailoring and supplementation of the security control baseline. Overlays may add or subtract security controls, or provide additional guidance regarding security controls, resulting in a set of security controls applicable to that system that is a combination of the baseline and overlay. Applying one or more overlays can reduce but does not necessarily eliminate the need for additional tailoring and supplementing controls.

If the use of multiple overlays results in conflicts between the application or removal of security controls, the AO (or designee), in coordination with the information owner/steward and the Risk Executive, will resolve any conflicts. If a control is added or removed by the application of an overlay, the SSP must reflect the change in the Security Requirements Traceability Matrix (SRTM). Further guidance on overlays and the application of them is provided within the overlay document itself.

Phase 3: Implement Security Controls

Implement Security Solutions

Security control solutions are implemented consistent with DHS enterprise architecture and information security architecture and apply best practices when implementing the security controls, to include employing system and software engineering methodologies, security engineering principles, and secure coding techniques. Security controls solutions must be designed and implemented the same as system functional requirements and plan for implementation throughout the entire SELC.

System design personnel to include security engineers should translate security control requirements into system specifications and ensure the successful integration ofthose capabilities into the system design. This includes ensuring that technical and performance requirements derived from the assigned security controls are included in requests for proposals and subsequent contract documents for design, development, production, and maintenance.

Best practices should be used in determining solutions for implementing the security control. Risk assessments may help inform decisions regarding the cost, benefit, and risk trade-offs in using one type of technology versus another for control implementation. The proposed system security design must be addressed in preliminary and critical design reviews. In many cases security control requirements may be satisfied through inheritance of common controls.

Mandatory configuration settings are established and implemented on information technology products in accordance with Federal, DHS, and Component policies. When available, the use of information technology products that have been tested, evaluated, or validated by approved, independent, third-party assessors should be considered.

Leveraging an Existing Authorization for Common Controls

A leveraged authorization is employed when a DHS Component ISSO intends to incorporate or connect their system to an existing DHS Enterprise/network/IT system and chooses to accept/inherit some or all the common controls documented in the DHS security authorization package. DHS Component ISSO must specifically document what controls are being inherited. The designated Security Control Assessor (SCA) for the DHS Component reviews the Enterprise/network/IS Common Controls. Otherwise, relevant documents from the security authorization package are reviewed to determine if the common controls satisfactorily fulfill the security requirements for the new system. Leveraging authorizations and reciprocal acceptance of security authorization packages for those common (inheritable) controls provided by DHS shall be employed to the maximum extent possible. A reciprocity memorandum should outline the agreement between the two IT systems/networks, with the approval of the respective AOs.

For common controls inherited by the system, project personnel should coordinate with the common control provider to determine the most appropriate way to implement them. Project personnel can refer to the catalogs prepared by common control providers when making determinations regarding the adequacy of common controls inherited by their systems. During implementation, it may be determined the common controls previously selected to be inherited by the system do not fully meet the protection needs of the system. For common controls that do not meet the protection needs of the systems inheriting the controls or when common controls are found to have unacceptable deficiencies, compensating controls to be implemented should be identified. System-specific or hybrid controls may also be utilized to supplement the common controls.

Document Security Control Implementation

As solutions are identified for implementing the required security controls the solutions must be documented in the SP and provide a functional description of the control implementation. The security control solution describes how system-specific, hybrid, and common controls are implemented. The description formalizes plans and expectations regarding the overall functionality of the IT system. The functional description of security control implementation includes planned inputs, expected behavior, and expected outputs where appropriate, typically for those technical controls that are employed in the hardware, software, or firmware components of the information system. Documentation of security control implementation allows for traceability of decisions prior to and after deployment of the information system. The documentation also addresses platform dependencies and includes any additional information necessary to describe how the security capability required by the security control is achieved at the level of detail enough to support control assessment. The SP is updated as the controls are implemented to ensure that the documented control implementation is consistent with the actual implementation.

Initial Security Control Assessment

Consistent with the flexibility allowed in applying the tasks in the RMF, Components conduct initial control assessments during system development and implementation. Security assessments determine the extent to which the controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the information system. Functional and initial security assessments occur as early as practicable in the system development life cycle, preferably during the development phase of the information system.

Conducting such assessments in parallel with the development and implementation phases of the SELC facilitates early identification of deficiencies and provides a cost-effective method for initiating corrective actions. Issues discovered during these assessments can be referred to authorizing officials for resolution.

Risk Assessment Update

Risk assessment of the initial security control assessment helps to identify how gaps in protection needs between systems and common controls affect the overall risk associated with the system, and how to prioritize the need for compensating controls to mitigate specific risks. The risk assessment report should be updated with information gained and reviewed to ensure none of the previously entered information has changed or otherwise become invalid. The updated risk report should be used to determine mitigation activities or unplanned control solutions where risk can be accepted. The results of the initial control assessments and updated risk assessment can also be used during the Authorize to Operation Phase to avoid delays or costly repetition of assessments. Assessment results that are subsequently reused in other phases of the SELC meet the reuse requirements established by the organization.

Phase 4: Assess Security Controls

An independent security control assessment is required once the system has been developed, security control solutions implemented and tested. The persons conducting the security control assessment should be independent of the system development and management structure overseeing the system.

Plan to Assess the Implemented Security Controls

The security assessment plan (SAP) provides the objectives for the security assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures. The assessment plan reflects the type of assessment the organization is conducting (e.g., developmental testing and evaluation, independent verification and validation, assessments supporting security authorizations or reauthorizations, audits, continuous monitoring, assessments subsequent to remediation actions).

The SAP must include:

- The scope of the assessment

- Controls to be tested or a justification as to why controls are not being tested

- Types of assessments to be conducted (e.g., interviews, tests, examinations)
- Tools to be used during the assessment
- Authorizations from relevant personnel

IACS facilitates the development of the security testing and evaluation plan based on the selected security controls.

Assess the Security Controls

Assessment procedures are used to verify that a security control has been properly implemented. NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, provides guidance for security control assessment procedures. Specific DHS procedures have been documented in the IACS that provides detailed overview of the requirements and associated test procedures included in the test plan for the information system. This saves time and effort required to manually search through the test plan for this information. It provides a detailed summary of applicable test procedures and an explanation of those tests that are not applicable due to equipment type, equipment scope, etc. The independent assessors should use the documented procedures to test each security control and capture the test results.

DHS Privacy Office is responsible for assessing privacy controls; however, all inquiries related to the testing should be directed to the Component Privacy office.

Prepare the Security Assessment Report (SAR)

The results of the security assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the Security Assessment Report. The security assessment report is one of the key documents in the security authorization package developed for Authorizing Officials. The security assessment report includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the SCA findings. The security assessment report is an important factor in an authorizing official's determination of risk to organizational operations and assets, individuals, other organizations, and the Nation.

The SAR must identify:

- The assessment team composition.
- Number of control tests performed.
- Number of passing and failing controls.
- Number of controls not applicable.
- Traceability – The number of failed controls that:

Conduct Initial Remediation Actions on Security Controls

The program personal should conduct a final review of the SAR, identify findings that can be remediated, and conduct initial remediation actions on security controls, as appropriate. Remediation activities should be retested, and the SAR updated. Program personnel should review the final SAR for accuracy and final security posture.

Residual Risk Assessment Report

Based on the SAR results a final residual risk assessment report should be prepared. Any known specific finding or vulnerabilities in the system should be documented in the risk assessment report, identifying the overall risk of the system finding and to guide the authorizing official in decision making. Any required waivers must be submitted in accordance to the waiver process and any risk planned for acceptance must be documented and appropriate approval gained.

Plan of Action and Milestones:

A Plan of Action and Milestones (POA&M) is mandated by the Federal Information Systems Modernization Act of 2014 (FISMA) as a corrective action plan for tracking and planning the resolution of IT system security weaknesses. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. DHS document "Process Guide for Plan of Action and Milestones," constitutes the core process for remediating control deficiencies in sensitive Department of Homeland Security (DHS) information systems.

The plan of action and milestones (POA&M), prepared for the Authorizing Official by the information system owner or the common control provider, is one of three key documents in the security authorization package and describes the specific tasks that are planned to:

(1) Correct any weaknesses or deficiencies in the security controls noted during the assessment
(2) Address the residual vulnerabilities in the information system.

The plan of action and milestones identifies:

(1) The tasks to be accomplished with a recommendation for completion either before or after information system implementation;
(2) The resources required to accomplish the tasks;
(3) Any milestones in meeting the tasks; and
(4) The scheduled completion dates for the milestones.

Phase 5: Authorize System to Operate

The authorize phase of the risk management framework (RMF) is where the AO decides whether to authorize the system for operation based on the security plan, security assessment report, and the plan of actions and milestones (POA&M). This provides the AO, at a minimum, the necessary information about risk impact.

Authorization Decision

In the Authorization Decision activity, the Authorizing Official (AO) reviews the security authorization package and makes the decision to grant or deny Authorization to Operate (ATO), Authority to Proceed (ATP), or Ongoing Authorization (OA).

The AO or DOA, with input from the Component Risk Executive make the Authorization Decision based on risk

POA&Ms associated with the security authorization must be documented, tracked, managed, and monitored.   An authorization letter must specify an expiration date that may be within three (3) years of the authorization date or as mentioned in the signed ATO letter. The authorization decision document contains the following information:

The Project Accreditation (with history) is used to indicate the authorization type granted to projects based on the results of the assessment effort, as well as to maintain a project's authorization history. The ATO/ATP/OA Letter provides the authority to operate the information systems or to use security controls inherited by those systems.

Terms and Conditions for the Authorization

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the ISSO or common control provider. The authorization termination date, established by the AO, indicates when the security authorization expires. The maximum time frame for a system authorization is three years from the signed authorization decision.

The primary stakeholders in this activity are the Risk Executive, System ISSM, Component CISO and with input from the Component SCA and System ISSO.

Authorization Termination Date

The date in which a system's authorization to operate expires and the system is no longer within operational compliance. The primary stakeholders in this activity are the Component ISSM and the Component CISO.

Phase 6: Monitor Security Controls

Information systems are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and operate. A disciplined and structured approach to managing, controlling, and documenting changes to an information system or its environment of operation is an essential element of an effective security control monitoring program. Strict configuration management and control processes are established by the organization to support such monitoring activities and manage any significant changes that may affect the security or privacy posture of the system. A significant change to the system may trigger an event-driven authorization.

Annual Assessment

Regular security assessments are also necessary after security authorization in order to maintain the security posture of the system and ensure controls continue to be implemented correctly since security controls tend to degrade over time. In addition, High Value Assets (HVA) may be selected for security assessment, led by DHS CISA, as outlined in BOD 18-02.

Annual Assessments are required as part of OMB circular A-130. Contingency plans must also be reviewed and updated and tested as part of this annual assessment.

CFO-designated systems are systems that impact the DHS general ledger and have a high visibility with senior officials at DHS. They are required to have a subset of security controls tested annually to ensure they are operating at an acceptable security posture."

Ongoing Authorization

Office of Management and Budget (OMB) Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems, states that "Our nation's security and economic prosperity depend on ensuring the confidentiality, integrity and availability of Federal information and information systems" and directs the National Institute of Standards and Technology (NIST) to publish guidance establishing a process and criteria for federal agencies to conduct ongoing assessments and ongoing authorization.

The Department of Homeland Security (DHS) addresses this issue through the implementation of its Ongoing Authorization (OA) program. The DHS Ongoing Authorization Methodology adheres to current guidelines and Federal requirements for continuous monitoring of data to promote ongoing system authorizations, risk-based decision-making, and near real-time awareness of the security state of the enterprise.

As stated in NIST 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, "initial system authorization is based on evidence available at one point in time, but systems and environments of operation change." To address the needs of constantly changing environments, DHS is implementing OA, which involves shifting from periodic to ongoing assessments and facilitates a continual state of awareness.

Upon completion of the security authorization process and attainment of an ATO, Components that have been accepted into DHS' Ongoing Authorization (OA) program have the option of entering a system into OA. As described in the DHS OA Methodology, OA is a time-driven and/or event-driven security authorization process whereby the Authorizing Official (AO) is provided with the necessary and sufficient information regarding the near real-time security state of the information system, including the effectiveness of the security controls employed within and inherited by the system, to determine whether or not the mission/business risk of continued system operation is acceptable.

The continual monitoring of security events and processes provides AOs the information needed to make risk determinations and risk acceptance decisions for OA systems more efficiently and effectively than the OMB A- 130 mandate of assessments every three years. It should be noted that the operations of the DHS OA Program are not necessarily in sequence with the steps of the Risk Management Framework (RMF) as they are defined in NIST SP 800-37 rev 2, but the RMF requirements are satisfied fully by OA processes and polices." For more information about ongoing authorization, please refer to the Ongoing Authorization Methodology guide.

Cybersecurity Reciprocity

Cybersecurity Reciprocity is the mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.

Reciprocity at DHS

DHS Components shall maximize the use of assessment results and authorizations of common information technology systems and software by other Components in earlier deployments. It is DHS policy that the security authorization process presumes acceptance of existing test and assessment results and authorization documentation. Accordingly, any DHS Component undertaking a security authorization effort shall determine if the system being evaluated has already been assessed, authorized and tested, and will proceed based upon existing assessment evidence. Cybersecurity Reciprocity is the default for security authorization of information systems already deployed within DHS.

Assessment and Authorization Documentation

Establishing trust relationships based on common, shared risk management principles and ensuring evidence regarding the security state of an information system is available to other organizations is the best approach to reciprocity.

This enables AOs from within the Department and other organizations to use the evidence to make cost-effective, risk-based decisions regarding the operation and use of an information system or the information it processes, stores, or transmits.

An ATO is evidence of a system being deployed in an operational environment based upon risk-based decisions that result from several factors in addition to security. The non-security factors that influence an authorization decision may differ across Components and Agencies and may lead to different authorization decisions.

Each DHS Component shall make all security authorization documentation available to other Components seeking to utilize reciprocity for that system or software.

Security Reciprocity Body of Evidence (BOE) Requirements

Each DHS Component shall make the BOE available to other Components. All BOE recipients should have the proper clearance, need to know, and storage facilities to handle and protect the BOE documentation. The BOE elements include but are not limited to the following:

- ATO Letter
- System Security Plan
- Privacy Threshold Assessment
- Privacy Impact Assessment (if applicable)
- POA&Ms
- Risk Assessment Report
- Risk Recommendation Letter
- Security Assessment Procedures
- Security Assessment Report
- System Inventory (Hardware and Software)
- Installation Procedures
- Configuration Information

Authorization Requirements

Any such cybersecurity assessment, authorization, and testing previously conducted by one DHS Component shall be evaluated prior to additional assessments or testing by another.

Assessments, authorizations, and tests by a DHS Component and other Federal Agencies/Departments shall be presumed to have been correctly completed, and the results shall be accepted by all Components as a basis for security authorization so long as the assessment is based on compatible hardware, software, services, and/or configurations. Any differences in the instance or environment, such as configuration differences, shall be documented, tested, and assessed by the requesting Component. A DHS Component may conduct additional testing to address unique conditions within its environment but is not authorized to repeat testing completed by another DHS Component. If a DHS Component asserts that the assessment, authorization, and testing completed by another was deficient in some manner and must be repeated, approval must be obtained from the DHS Chief Information Security Officer (CISO) prior to any additional assessment, authorization, or testing.

All DHS authorizations, including Reciprocity Authorizations, shall be performed according to the latest System Security Authorization Process Guide, policies, standards and guidance applicable to DHS Sensitive Information Systems, including those implemented pursuant to the Federal Information Security Modernization Act of 2014 ("FISMA"), all relevant Federal Information Processing Standards, and OMB Circular A-130 when designing, developing, operating, maintaining and disposing of federal information systems including information systems for operational technology. When using cloud computing to provide information systems or services, all DHS authorizations, including Reciprocity Authorizations, shall adhere to FedRAMP security authorization requirements and continuous monitoring requirements as described in NIST Special Publication (SP) 800-137 and governed by the FedRAMP Continuous Monitoring Strategy Guide and FedRAMP Incident Communications Procedures.