Homeland Security

System Security Authorization Process Guide

Version 14.1

April 4, 2019

Document Change History

Version	Date	Description
14.0	June 15, 2018	Wholly revised to align with current authorities.
14.1	April 4, 2019	Added Authority to Proceed and External Information System guidance

Contents

.

1.0 INTRODUCTION

Under the authority of the Department of Homeland Security (DHS) Chief Information Officer (CIO), the Chief Information Security Officer (CISO) is charged with the primary responsibility for ensuring compliance with Federal Information Security Modernization Act (FISMA 2014), Office of Management and Budget (OMB) A-130, National Institute of Standards and Technology (NIST) publications, and all other applicable laws, directives, and policies. This document defines the DHS Security Authorization process for information systems operated within the Department.

The SA process applies certain engineering activities and tasks based on NIST Special Publication (SP) 800-160 and uses the Risk Management Framework (RMF) from NIST SP 800-37. These steps include conducting the activities of organizational preparation, security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. This process helps ensure that management of information system-related security risks is consistent with the DHS mission and business objectives and the overall risk strategy established by the Department and Components.

2.0 BACKGROUND

Security Authorization (SA) is the authorization given by an Authorizing Official (AO) for operation of an information system, and by which the AO explicitly accepts the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

SA involves comprehensive testing and evaluation of a system's security controls from conceptualization and initiation of the System Engineering Life Cycle (SELC) through acquisition of components and adhering to the NIST Risk Management Framework (RMF), culminating with the system's entry into production. SA addresses external threats and risks, varying development processes, and software and hardware security safeguards; considers procedural, physical, and personnel security measures; and establishes the extent to which a system's architecture, configuration, and implementation meet a specified set of security requirements throughout its life cycle. SA also considers the procedural, physical, and personnel security measures employed to enforce information security policy.

An information system must be granted an Authority to Operate (ATO) before it first becomes operational, and it must be re-authorized whenever changes are made that affect the potential level of risk of operating the system. Ongoing Authorization (OA) will be discussed in later sections of this document; it allows for a continuous assessment and reauthorization process. An SA typically begins at the requirements gathering phase of SELC and an ATO is required before the system is made *operatio*n*al*. The term *operational* means that the information system has begun processing real or live data.

AOs may grant an Interim Authorization to Operate (IATO) for information systems that are undergoing developmental testing or are in a prototype phase. The AO may initially grant an IATO for a maximum duration of six (6) months and may grant a single six (6) month extension.

IATOs are not authorized for operational systems. IATOs are typically granted in the for a non-operational development information system testing with production data. In general, DHS does not recognize IATOs. AOs may grant an IATO for systems processing operational and sensitive data as part of an Agile Development methodology.

AOs may grant an Authorization to Proceed (ATP) for information systems that are in initiation, undergoing development testing, or are in a prototype phase of development. AOs may also grant an ATP for systems processing operational and sensitive data as part of an Agile Development methodology. The AO may grant an ATP for a maximum duration of one (1) year. When an ATP is granted, the system will enter the SELC *Implementation* phase and become reportable on the FISMA Scorecard. It can also initiate processing of production data. One year from the time the ATP is issued, all remaining security control documentation and a full assessment must be completed as required by the official ATO process. If an ATO is not received within one year, the system will be non-compliant and the ATP will be revoked, thereby affecting the FISMA Scorecard. Systems approved for ATP will not be allowed to move into the Ongoing Authorization program unless a full assessment has been completed and an ATO has been granted.

For systems using the legacy three (3) year ATO process, conducting a re-authorization is the same process used to conduct the initial security authorization. The primary difference is that an initial security authorization should be started early in the SELC process while re-authorization will usually begin four (4) to six (6) months before the current ATO expires. This timeframe assumes that resources are available to start the security authorization process. For systems in the OA program, reauthorization may occur on a time or event driven basis and is documented by the OA Recommendation Letter as required by the DHS OA Methodology; repetition of only certain steps or phases of the RMF is involved.

3.0 PURPOSE

The purpose of this document is to provide practical guidance for conducting a DHS SA. NIST guidance, OMB guidance and directives, DHS security policies, guidance and directives, and all applicable laws, directives, and policies.

4.0 SCOPE

This guide applies to all unclassified DHS systems, including General Support Systems (GSSs), Major Applications (MAs) in DHS FISMA Inventory. All GSSs and MAs must be assessed and authorized in accordance with the process defined in this guide. All sub-systems and minor applications must be documented in the security authorization package of an associated GSS or MA.

The process for assessing and accrediting National Security Systems (NSS) is outside the scope of this guide.

5.0 ROLES AND RESPONSIBILITIES

Within DHS guidelines, each Component, organization, and system Team determines its own internal procedures for conducting a security authorization. In some cases, security authorizations are conducted by ISSOs. In other cases, a system Team may use contractors hired specifically to conduct the security authorization or Components may provide a dedicated security authorization group for use within the Component. This section lists personnel who have key roles in the SA process and briefly describes the duties of each.

5.1 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 SA package, and grants or denies an 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.

5.2 Chief Information Security Officers (CISO) and Information System Security Managers (ISSM)

The DHS Chief Information Security Officer (CISO) provides overall guidance for conducting SAs.

CISOs or Information System Security Manager (ISSM) provides specific guidance for the SA process within the Component and serves as the Security Control Assessor (SCA) unless someone else is designated.

5.3 DHS Inventory Management (IM) Team

FISMA requires development, maintenance, and updating an inventory of information systems operated by DHS or under its control. This inventory also includes identification of the interconnections between each system and all other systems or networks, including those not operated by or under the control of the Department. The DHS Information Technology (IT) system inventory is also used to support information resources management; IT planning, budgeting, and acquisition; the monitoring, testing, and evaluation of information security controls; and the preparation of the index of major information systems required by the Freedom of Information Act (FOIA). The DHS CISO, and subsequently the IM Team within OCISO, is responsible for oversight and ensuring compliance with FISMA throughout DHS, to include developing and maintaining a Department IT system inventory.

The DHS IM Team's role consists of two primary functions: performing routine change management and conducting the annual refresh process.

DHS Components are required to submit a Change Request form to the IM team any time the SELC status or centrally managed data fields of an information system owned or operated by DHS changes. It is the IM team's responsibility to process change requests and update the

Information Assurance Compliance System (IACS) reporting system. More information can be found in the DHS FISMA System Inventory Methodology.

The IM Team also conducts an annual review of all DHS information systems. This months-long activity is called the FISMA Inventory Annual Refresh. The Annual Refresh is an opportunity for Components to holistically review and update their inventory and for the System Owner to clarify any discrepancies found through independent reviews. More information may be found in the FISMA Inventory Methodology guide.

5.4 Security Control Assessor (SCA)

The SCA is a senior management official whose responsibilities include certifying the results of the security control assessment. An SCA is assigned in writing to each information system by the Component CISO. 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 or not 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 Component CISO is normally the SCA when no other person has been officially designated.

The SCA ensures that testing of security controls are documented in the requirements traceability matrix (RTM). The RTM is created automatically in IACS, 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, as long as test results are reviewed by an independent source to validate 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 1 illustrates the information hierarchy among various stakeholders needed to complete the Security Authorization process.

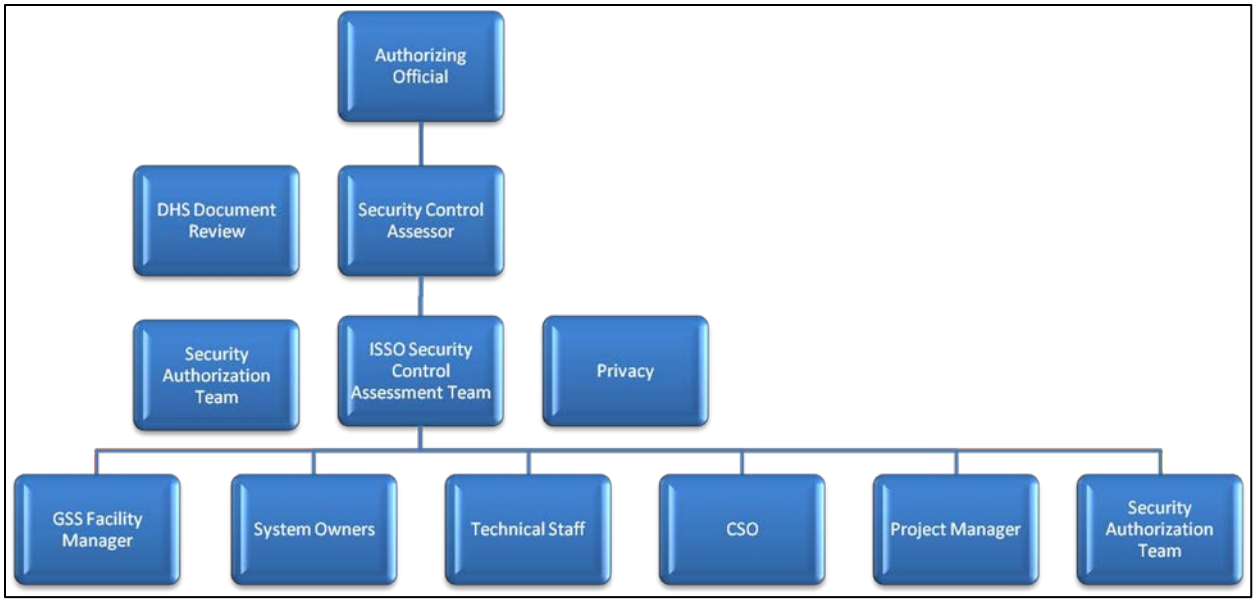

Figure 1: Information hierarchy of stakeholders in the security authorization process

5.5 Security Authorization (SA) Team

The SA 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 SA team may also conduct the security assessment depending on the need for separation of duties.

The SA team needs access to the DHS SA IACS tool.

Figure 2 shows the different stakeholders that must be engaged in order to conduct an efficient security authorization.

Figure 2: Security Authorization Team Stakeholders

5.6 Threat Intelligence Gathering Entity

OCISO National Security Systems Division (NSSD) is the threat intelligence gathering entity. NSS gathers data from various sources and analyzes that data to determine to relevance the organizations and the disparate missions of DHS Component entities.

5.7 DHS CISO Council

The CISO Council reviews the threat analysis and recommendations provided by the threat data gathering entity (NSSD) and uses that information to inform and assist Components with determining the level of risk to systems and appropriate categorization of information systems.

5.8 Component CISO or Designee

The organization's 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.).

5.9 Information System Security Manager (ISSM)

Components that are not required to have a fulltime CISO have a fulltime ISSM. The ISSM is designated in writing by the Component CIO, with the concurrence of the DHS CISO.

The ISSM plays a critical role in ensuring that the DHS information security program is implemented and maintained throughout the Component.

Component ISSMs:

- Oversee the Component information security program
- Ensure that the Component CIO and DHS CISO are kept informed of all matters pertaining to the security of information systems
- Ensure that all communications and publications pertaining to information security, including updates to the 4300 Policies and Handbooks, are distributed to the ISSOs and other appropriate persons within their Component
- Validate all Component information system security reporting
- Consult with the Component Privacy Officers or Privacy Points of Contact (PPOC) for reporting and handling of privacy incidents
- Manage information security resources including oversight and review of security requirements in funding documents
- Test the security of the Component's information systems periodically
- Implement and manage a Plan of Action and Milestones (POA&M) process for remediation by creating a POA&M for each known vulnerability
- Ensure that ISSOs are appointed for each Component-managed information system
- Ensure that weekly incident reports are forwarded to the DHS 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 Secure Baseline Configuration Guides (DHS 4300A Sensitive Systems Handbook)
- Develop and publish procedures for implementation of DHS information security policy within the Component
- Implement DHS information security policies, procedures, and control techniques to address all applicable requirements
- Ensure training and oversight for personnel with significant responsibilities for information security
- Oversee the SA process for the Component's 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
- Ensure that enterprise security tools are used
- Ensure that ISSOs monitor and manage the information security aspects of supply chain risks
- Ensure that ISSOs adopt software assurance principles and tools

5.10 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. Component ISSOs:

- Ensure that security requirements for the major application or general support system are being or will be met
- Ensure that requests for security authorization of computer systems are completed in accordance with the published procedures
- Ensure that protective measures such as deadbolt locks on doors, placement of electrical wiring, etc. as countermeasures for physical security threats, are in place
- 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 within the program and development offices or field site facility
- Coordinate the development of a Contingency Plan and ensure that the plan is tested and maintained
- Ensure that risk analyses are completed to determine cost-effective and essential safeguards
- Ensure preparation of security plans for sensitive systems and networks
- 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 IT security personnel for preparation of reports to higher authorities concerning sensitive and/or national security information systems

5.11 System 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.

5.12 Program 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).

5.13 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.

5.14 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.

5.15 Business 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.

5.16 Privacy Office

The Chief Privacy Officer (CPO) is responsible for the implementation of NIST SP 800-53 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.

For DHS, the Privacy Office 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.

5.17 DHS Document Review Team (DR)

The DHS Document Review (DR) Team reviews and validates security authorization packages after they have been completed in IACS. Additional information may be found in Appendix A.

6.0 RISK MANAGEMENT FRAMEWORK AND THE SELC PROCESS

The RMF provides a disciplined and structured process that integrates information security and risk management activities with SELC. The RMF operates primarily at the information system level, but when aligned with system security engineering processes, as defined in NIST SP 800-160, it can extend to tasks and activities, including organizational risk, that are provisioned as

organizational level processes and provide a bridge to the more system-specific elements of the framework. The process is thus applicable throughout a system's life cycle and encompasses all types of systems (i.e., new, modified, upgraded, etc.) and the security considerations applicable to their engineering requirements. Communication between the organization and the system owner are critical in maintaining a risk management strategy and ensuring that events impacting risk are accounted for. Thus the RMF has been updated (Figure 3) to include the "organization preparation" with the more familiar categorize, select, implement, assess, authorize, and monitor tasks. More information can be found in the draft NIST SP 800-37 rev2, "Risk Management Framework for Information Systems and Organizations."

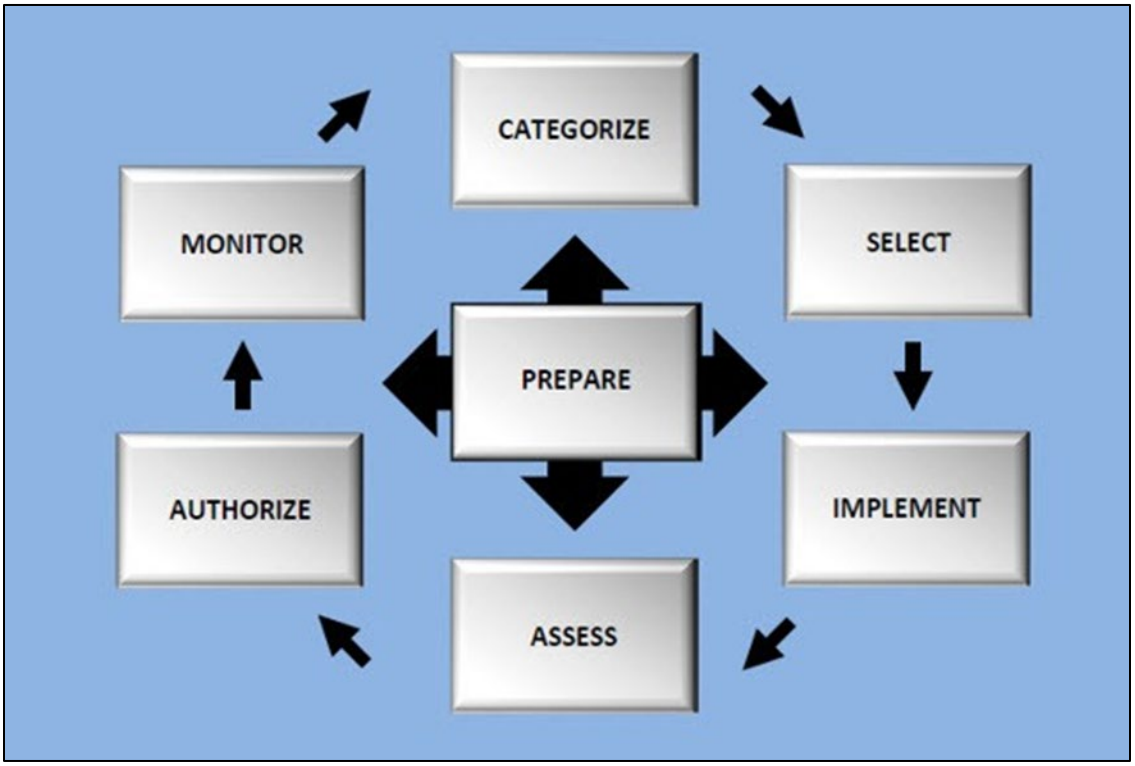

Figure 3: The Risk Management Framework

6.1 Prepare

This initial step of the RMF is used to provision and make available security related organizational level processes and activities that provide a bridge to use of the system- specific tasks of the RMF. As illustrated in Figure 3, the Prepare task allows for development and use of steps such as risk and privacy assessment during the SELC process that may be revisited as the system matures during later task in the RMF process. Other Prepare tasks such as development of a risk management strategy are created at this time but not necessarily documented within the SA tool.

The current SA tool's workflow is structured to align the RMF with the NIST Cybersecurity Framework, the system security engineering process as defined in NIST SP 800- 160, SP 800-37 and SP 800-39. Organization and mission level steps included in the Prepare task are as follows:

- Individuals are identified and assigned key roles for executing the Risk Management Framework.
- A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established.
- An organization-wide risk assessment is completed or an existing risk assessment is updated.
- Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles are established and made available.
- Common controls that are available for inheritance by organizational systems are identified, documented, and published.
- A prioritization of organizational systems with the same impact level is conducted.
- An organization-wide strategy for monitoring control effectiveness is developed and implemented.

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 classified as General Support Systems (GSS) or Major Applications (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.

An External Information System (EIS) is an information system or set of components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness.

EISs include:

- Personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants)

- Privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); information systems owned or controlled by nonfederal governmental organizations
- Federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations

Before a system can be added to IACS, a request must be submitted to the DHS Inventory team with the Inventory Change Request Form. The Inventory Team will review and process the form and assign a unique FISMA ID to the system and the system will be added in IACS. Refer to the DHS Inventory Methodology for more information.

Certain Capital Planning and Investment Control (CPIC) information is entered and maintained in IACS. This includes the IT name and Unique Investment Identifier (UII Code) from DHS Enterprise Business Management Office (EBMO) and synchronization with INVEST Business Case/Portfolio Reporting. The Component's CPIC administrator maintains this data.

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.

Organizational risk provides the context (frame) for which everything else is assessed. This is usually provided in policy (i.e. DHS Sensitive Systems Policy Directive 4300A), business continuity plans, disaster 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, 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. It is imperative the ISSO be informed and incorporate this frame into threat/risk assessments.

6.1.1 Risk Assessment (RA)

An RA is a formal analysis of an information system used to identify potential vulnerabilities to the system, determine the extent of the potential threat and the risk to the system throughout its life cycle. Additionally, an RA is used to determine whether existing countermeasures and safeguards adequately reduce the probability of loss to an acceptable level and help validate the need for additional cost-effective countermeasures. The *DHS 4300A Sensitive Systems Handbook* requires that an RA be conducted to provide information supporting the AO's decision to

formally authorize the system to operate. This document follows the guidance provided in the DHS Sensitive Systems Policy Directive 4300A and the 4300A *Handbook*. For further understanding of risk management, refer to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Guide for Conducting Risk Assessment.

RA includes identifying environmental, human, and natural threats, and should be started at the very beginning of the SELC process and updated as the system is developed. It should incorporate the data center disaster recovery plan and document risk at the facility as well as the risks identified at the Component and DHS level.

Overarching vulnerabilities are identified in the risk assessment based on the hardware, software, and firmware used in the system. These vulnerabilities are usually addressed at the Component level and impact overall security categorization. The comprehensive list of vulnerabilities included from scans are identified in the Security Assessment Report (SAR).

The RA also identifies security controls that are addressed at the DHS and Component level (through common controls typically). These security controls have a common implementation strategy designed to reduce the impact and likelihood of a threat exercising a vulnerability.

Common control catalogs are available for use in IACS.

6.1.2 System Information

It is vitally important to define the system as completely as possible and as early as possible in the development of the system. As the system is developed, the information is updated and documented in a Security Plan (SP). This provides flexibility to make changes to the system throughout the RMF. The information described here is part of the SP but should be documented as early as possible and revised as the system is developed.

6.1.3 System Boundary

The process of uniquely assigning information resources to an information system defines the security boundary for that system. If a set of information resources is identified as an information system, the resources should generally be under the same direct management control. Direct management control does not necessarily imply that there is no intervening management. The actual boundary is defined by the Components and communicated to the DHS FISMA Inventory Management Team. For more information on determining boundaries, please see the DHS FISMA Inventory Methodology.

All hardware, software, and firmware is documented as part of the system boundary. Although the RMF makes the assumption that all technical requirements are finalized, 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.

Hardware contains all the physical equipment in the system. This generally refers to servers, workstations, routers, switches, specialized hardware such as network sensors including Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Internet of Things (IoT).

Software is a collection of programs designed to direct the operation of an information system. This is generally categorized as operating systems, database management systems, web servers, network monitoring software, and specialized application software.

Firmware is a microprogram stored in non-volatile. It is a specific type of software that provides control for specific hardware. Since it controls devices, it poses a security risk to the information system. All firmware for all devices should be documented and updated as necessary.

The internal and external connections of the information system are documented as well. This includes the ports, protocols, and services used to connect and transfer data between devices and software applications. External connections should be documented via an interconnection security agreement, memorandum of understanding, or memorandum of agreement. This documentation includes the security responsibilities of all parties who share the information contained in the system. As part of this documentation, a data flow diagram should be created and maintained as well as a network diagram documenting the devices and their interconnections.

6.1.4 System Environment

The system environment is the operating environment where the information system resides, including both physical and technological considerations. Technological considerations are defined in the interrelationship of hardware, software, and firmware. The physical considerations are part of a data center and include: the geographic location of the data center, the climate of the data center, both inside and outside, the data center's procedures for physical access, etc. This information is pertinent for both the RA and the SP.

6.1.5 Project Personnel

The project personnel are the people who have responsibilities for assessing the information system. They include the AO, ISSO, system owner, etc. This information is usually known in advance of the technical requirements and should be documented as early as is feasible and updated continuously.

6.1.6 System Users

System users are identified and documented in the SP, allowing for the creation and tracking of roles and permissions for specific categories of users. This includes server administrators, database administrators, maintenance engineers, and different roles of application users such as auditors, account administrators, and end users. These are categories of users who will access and maintain the information system. These system users, and their minimum qualifications, are defined by the mission, laws, regulations, policies, and information security best practices.

6.1.7 ISSO Designation Letter

All ISSOs must be designated in writing following the guidance in *DHS 4300A Sensitive Systems Handbook* Attachment C. ISSO letters define duties and responsibilities and are usually signed by the System Owner. ISSO letters must be updated whenever a change occurs. The designated ISSO should be consistently identified in three places: in the ISSO letter, in the SP and in IACS.

6.1.8 Ports, Protocols & Services

Ports, protocols and services are the communication pipelines of the information system. The routes used should be documented using the host port, the destination port (e.g. port 443), the protocol used (e.g. TCP), and the service using the ports and protocol. This should include connections between database servers and application servers, local network connections for backup or system mirroring, and flow of routine traffic (e.g. email, etc.).

6.1.9 Analyze Risk Elements

Analyzing, assigning, and mitigating risk is an ongoing activity throughout the life-cycle of the system. A risk element is a risk-based item requiring a risk-based decision. Risk elements come from a failed test, a RA, SP or any source that can introduce risk to the system. Risk elements should be documented when they are discovered.

6.2 Categorize

The purpose of this step is to guide and inform subsequent risk management processes and tasks by determining the adverse impact or consequences to the organization with respect to the confidentiality, integrity, and availability of organizational systems and the information processed, stored and transmitted by those systems.

Security categorization is carried out by the system owner and the ISSO in collaboration with various organizational personnel. Information systems are categorized by the mission that the systems support.

6.2.1 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.

6.2.2 Security Categorization

Security categorization is the process of applying risk to an information system. The mission and business functions are used to select system data types. System data types are specific lines of business that are mapped to the DHS Business Reference Model (BRM). The 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 are selected using the DHS BRM to determine 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.

Once a final determination has been made for the security impact of the system, the security controls supporting it may be selected.

6.3 Privacy Requirements

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 makes determines 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.

6.4 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. The DHS CFO publishes an updated comprehensive list of CFO-designated Systems every fiscal year and distributes that list to Component CFOs, CIOs, and CISOs. The list may change from year to year depending on a number of factors. CFO-designated systems are identified every year by the DHS Inventory Team from the list issued by the DHS CFO.

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."

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

Financial systems are not necessarily on the CFO-designated list; their inclusion, depends on their relevance to their overall impact on the financial statement.

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.

6.5 Select

Once the security categorization is performed for each security objective, the DHS baseline of controls is applied. DHS applies both NIST security controls and DHS 4300A requirements. Although this baseline provides a minimum set of controls, the Component, AO, system owner, and ISSO may determine that more or more stringent controls are necessary to mitigate risk to an acceptable level. Other considerations should also be taken into account 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 FIPS 199 categorization for each security objective, the mission of the organization, the relationship of the information system to other systems, for example common controls, interconnection security agreements, Memorandums of Agreement (MOA) and Memorandums of Understanding, 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.

The selected security controls are documented in a system security plan (SP). The SP contains an overview of the security requirements for the information system in sufficient detail to determine that the security controls selected would meet those requirements. The SP, in addition to the list of security controls to be implemented, describes the intended application of each control in the context of the information system with sufficient detail to enable a compliant implementation of the control.

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

6.5.1 Requirements Questionnaire

The requirements questionnaire is a tool in IACS that assists in tailoring security control applicability. The questions are answered with a simple yes or no and the results are used to decide the applicability of controls related to the question. DHS 4300A controls must be addressed for all Sensitive but Unclassified (SBU) systems.

6.5.2 Organizationally Defined Requirements

Security controls and control enhancements containing embedded parameters (i.e., assignment and selection statements) give organizations the flexibility to define and review specific organizational requirements.

This step defines the requirement assignment questions that are used to collect specific information that varies from organization to organization. All of the questions on this page are based on DHS guidance (e.g., 3 attempts, 90 days). The answers are added automatically to the associated requirement, identified by the paragraph number in the brackets at the end of the question. The answers replace existing text, such as [Assignment: organization-defined time period].

6.6 Implement

Security control implementation is described, as appropriate, in the SP, and provides a functional description of control implementation. Security control documentation describes how system-specific, hybrid, and common controls are implemented. The documentation formalizes plans and expectations regarding the overall functionality of the information 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 sufficient to support control assessment.

After the security controls are documented in the SP, they are implemented in accordance with their descriptions in the SP. Best practices are used when implementing security controls.

The descriptions include system and software engineering methodologies, security engineering principles, and secure coding techniques. 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. In addition, the system owner and ISSO ensure that mandatory configuration settings are established and implemented on information technology products in accordance with Federal, DHS, and Component policies. When available, the system owner and ISSO should consider the use of information technology products that have been tested, evaluated, or validated by approved, independent, third-party assessors. The SP is updated as the controls are implemented to ensure that the documented control implementation is consistent with the actual implementation.

6.6.1 Security Plan (SP)

A security plan is a formal document which provides an overview of the security requirements for an information 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, and POA&Ms for implementing security controls. Procedures should be in place outlining who reviews the plans, keeps the plan current, and follows up on planned security controls. In most cases, this is the ISSO. In addition, procedures should require security plans be

developed and reviewed prior to proceeding with the security authorization process for the system.

All equipment (hardware) within an information system is 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. This information is the basis of building tests supporting the security controls.

IACS allows hardware and equipment to be organized by groups. This provides a process for organizing and categorizing specific types of hardware. It also allows grouping based on similar configuration settings, 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.

6.6.2 Security Controls

At this point, the listed security controls are implemented in the security plan. The control implementation is consistent with the DHS and Component enterprise architecture and the associated security and privacy architectures. Controls providing a specific security or privacy capability are only allocated to those system components that require the specific security or privacy capability and should be noted in the plan. The security controls implementation should also be described in multiple tiers or layers of the information system based on software layers. The security categorization, the privacy risk assessment, the security and privacy architectures, and the allocation of controls work together to help achieve a suitable balance between security and privacy protections and the mission-based function of the system.

Best practices are used when implementing controls, including systems security and privacy engineering methodologies, concepts, and principles. Risk assessments guide and inform decisions regarding the cost, benefit, and risk trade-offs in using different technologies or policies for control implementation. ISSOs also ensure that mandatory configuration settings are implemented on system components in accordance with federal, DHS, and Component policies. When there is not direct control over what controls are implemented in a system component, for example, in commercial off-the-shelf products, consider the use of system components that have been tested, evaluated, or validated by approved, independent, third-party assessment facilities (e.g., NIST Cryptographic Module Validation Program Testing Laboratories, National Information Assurance Partnership Common Criteria Testing Laboratories) or other Components within DHS.

For common controls inherited by the system, coordinate with the common control provider to determine the most appropriate way to implement them. System owners 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, the system owners identify compensating controls to be implemented. System owners can supplement the common controls with system-specific or hybrid controls to achieve

the required protection for their systems or accept greater risk with the acknowledgement and approval of the authorizing official. Risk assessments may determine 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. Control implementations must meet the criteria established under Appendix A, "Document Methodology." Controls that are "Planned" or "Not Implemented" must identify the applicable POA&M number.

Consistent with the flexibility allowed in applying the tasks in the RMF, Components conduct initial control assessments during system development and implementation. 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. The results of the initial control assessments can also be used during the authorize step 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. For systems in Ongoing Authorization, the timeframe of control reassessments are determined by a risk assessment using the likelihood of a vulnerability being exploited. This is documented in a control allocation table (CAT) and must be periodically reviewed.

6.6.3 Contingency Plan (CP)

Contingency planning refers to interim measures to recover information system services 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. These measures are documented in a contingency plan.

The intent of a contingency plan, as described by Section 3.5.2 of the DHS 4300A Sensitive Systems Handbook, is to ensure the availability of critical information systems under all circumstances. A contingency plan provides for capability to respond to emergencies, to recover from them, and to resume normal operations, possibly at an alternate location, in the event of emergency, system failure, or disaster.

Specific control requirements for emergency situations, and level of effort expended, are determined based on the information system's security categorization. The level of resources for the Contingency Plan is based on the security categorization for the availability security objective:

- For systems with a **low impact for availability**, the system owner can determine the Contingency Plan format and content that is appropriate for the system and its environment. The Contingency Plan generated in the IACS automated Security Authorization tool can also be used.
- For systems with a **moderate impact level for availability**, the default Contingency Plan template in IACS should be used.
- Systems with a **high impact level for availability** should develop a rigorous Contingency Plan. The template to be used for such a plan can also be found in IACS. The high impact plan can be received in IACS when creating a package, by answering "Yes" to additional documents in the questionnaire.

Please note it is important for the CP to have as much information as possible to restore the information system. In the event of an emergency, it is likely the CP is the only document available and it should have all the information necessary to restore the system without referring to another document.

There are seven steps involved in developing a CP. They are as follows:

(1) Develop the contingency planning policy statement. A formal policy provides the authority and guidance necessary to develop an effective contingency plan.

(2) Conduct the business impact analysis (BIA). The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes. A template for developing the BIA is provided to assist the user.

(3) Identify preventive controls. Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.

(4) Create contingency strategies. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.

(5) Develop an information system contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.

(6) Ensure plan testing, training, and exercises. Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.

(7) Ensure plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

A CP addresses three distinct phases from the moment of significant system disruption to full restoration of system functionality—activation/notification, recovery, and reconstitution. The Activation/Notification Phase describes the process of activating the plan based on outage impacts and notifying recovery personnel. The Recovery Phase details a suggested course of action for recovery teams to restore system operations at an alternate site or using contingency capabilities. The final phase, Reconstitution, includes activities to test and validate system capability and functionality and outlines actions that can be taken to return the system to normal operating condition and prepare the system against future outages.

The Activation/Notification Phase defines initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan. At the completion of the Activation and Notification Phase, CP staff (identified and maintained within the CP) will be prepared to perform recovery measures to restore system functions.

The notification strategy should define procedures to be followed in the event that specific personnel cannot be contacted. Notification procedures should be documented clearly in the CP. Copies of the procedures can be made and located securely at alternate locations. A common manual notification method is a call tree. This technique involves assigning notification duties to specific individuals, who in turn are responsible for notifying other recovery personnel. The call

tree should account for primary and alternate contact methods and should discuss procedures to be followed if an individual cannot be contacted.

Formal recovery operations begin after the CP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location. At the completion of the Recovery Phase, the information system will be functional and capable of performing the functions identified in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation at an alternate system, or relocation and recovery at an alternate site.

To facilitate Recovery Phase operations, the CP should provide detailed procedures to restore the information system or components to a known state. Given the extensive variety of system types, configurations, and applications, this planning guide does not provide specific recovery procedures.

The Reconstitution Phase is the third and final phase of CP implementation and defines the actions taken to test and validate system capability and functionality. During Reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. This phase consists of two major activities: validating successful recovery and deactivation of the plan.

At the successful completion of the validation testing, CP personnel will be prepared to declare that reconstitution efforts are complete and that the system is operating normally. This declaration may be made in a recovery/reconstitution log or other documentation of reconstitution activities. The CP Coordinator, in coordination with the system owner, ISSO, Component CISO, and with the concurrence of the Authorizing Official, must determine if the system has undergone significant change and will require reauthorization.

6.6.4 Contingency Plan Test (CPT)

A CP should be maintained in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities within the plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in the environment specified in the CP. In addition, as indicated in Step 4 (Assess Security Controls) of the RMF, the effectiveness of the information system controls should be assessed by using the procedures documented in NIST SP 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems." NIST SP 800-84, "Guide to Test, Training and Exercise

Programs for Information Technology Plans and Capabilities," provides guidelines on designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events so that organizations can improve their ability to prepare for, respond to, manage, and recover from adverse events. While the majority of TT&E activities occur during the Operations phase, initial TT&E events should be conducted during the Implementation phase of the SELC to validate CP recovery procedures.

Components must conduct contingency plan testing events at least annually, following organizational or system changes, or the issuance of new testing guidance, or as otherwise

needed. Execution of CPT events assists organizations in determining the plan's effectiveness, and that all personnel know what their roles are in the conduct of each information system plan. CPT event schedules are often dictated in part by organizational requirements.

CPTs must document that the appropriate exercise was conducted (call tree, table top, full functional exercise). A low availability should have the call tree tested and updated. A moderate availability should conduct a tabletop exercise and a high availability should conduct a full functional exercise. A full functional exercise requires that a portion of the system be taken offline and brought back into operation as part of a simulation. If the appropriate exercise cannot be conducted, the CPT must contain a justification and reference a POA&M number and/or waiver number. Full functional exercises may not be required for Federal Risk and Authorization Management Program (FedRAMP) systems if the applicable CP controls are fully or partially inherited from the FedRAMP authorized Cloud Service Provider (CSP).

6.6.5 Configuration Management Plan (CMP)

Configuration Management (CM) comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.

A Configuration Management Plan (CMP) is a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems. The basic parts of a CMP include:

- Change Control Board (CCB) – Establishment of and charter for a group of qualified people with responsibility for the process of controlling and approving changes throughout the development and operational lifecycle of products and systems; may also be referred to as a change control board;
- Configuration Item Identification – methodology for selecting and naming configuration items that need to be placed under CM;
- Configuration Change Control – process for managing updates to the baseline configurations for the configuration items; and
- Configuration Monitoring – process for assessing or testing the level of compliance with the established baseline configuration and mechanisms for reporting on the configuration status of items placed under CM.

The CMP ensures that configuration and control changes to the system are monitored, evaluated, and impacts are assessed prior to implementation.

6.7 Security Assessment

Conducting security assessments in parallel with the development/acquisition and implementation phases of the life cycle permits the identification of weaknesses and deficiencies early and provides the most cost-effective method for initiating corrective actions. Issues found during these assessments can be referred to authorizing officials for early resolution, as appropriate. The results of security assessments carried out during system development and implementation can also be used (consistent with reuse criteria) during the security authorization process to avoid system fielding delays or costly repetition of assessments.

Security assessments determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Security assessments occur as early as practicable in the system development life cycle, preferably during the development phase of the information system. 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.

6.7.1 Security Assessment Plan (SAP)

The security assessment plan 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

6.7.2 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:
  - Require remediation within 12 months via POA&Ms
  - Require approved waivers signed by DHS CISO for any risks waived
- Residual level of risk.
- SCA recommendation to the AO.

All control failures will be documented and mitigated in accordance with this guide.

6.7.3 Test Plan & Results/Requirements Traceability Matrix

The project test matrix provides a 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. All test results should be recorded in the Test Plan and Results section of IACS.

The results of assessments must be documented under Test Plan and Results and the Security Authorization Report (SAR). The SAR should correspond with the Test Plan and Results (e.g. if the SAR states 50 controls failed, those controls should be documented as failures under Test Plan and Results).

6.7.4 Analyze Risk Elements

The Analyze Risk Elements step presents a list of information system's risk elements and provides the tools and information required to review and analyze them. A risk element is an item from a failed test or a user-defined item that could potentially impact the security of the system based upon threats and vulnerabilities to the information system. Risk elements that are not accepted are used to create POA&Ms.

6.7.5 POA&M Elements

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 information 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. The 4300A Attachment H "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. POA&Ms are mandated as part of the essential documents for an ATO.

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.

The plan of action and milestones is used by the authorizing official to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment. All security weaknesses and deficiencies identified during the security control assessment are documented in the security assessment report to maintain an effective audit trail. Organizations develop specific plans of action and milestones based on the results of the security control assessment and in accordance with applicable laws, Executive Orders, directives, policies, standards, guidance, or regulations. Plan of action and milestones entries are not required when weaknesses or deficiencies are remediated during the assessment or prior to the submission of the authorization package to the authorizing official.

6.8 Authorize

The authorize phase of the risk management framework (RMF) is where the AO makes a decision whether or not 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.

6.8.1 Document Review

DHS document review (DR) implements a rigorous set of quality standards across all DHS Security Authorization (SA) packages to ensure applicable DHS and NIST controls have been properly documented. The DR team conducts its review based on a DR checklist of items. The SA documents are assessed based on this checklist. All SA packages must have DR approval before the system is in compliance on the DHS Information Security Scorecard.

DR is not meant to hold up the Authorization process; however, it requires actions that need to be taken to give the AO assurance the SA package meets the standards DHS has set out in the DR methodology.

6.8.2 Authorization Decision

In the Authorization Decision task, the Authorizing Official (AO) reviews the security authorization package and make the decision to grant or deny authorization to operate (ATO) or Authority to Proceed (ATP). 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 Letter provides authorization to operate information systems or to use security controls inherited by those systems.

6.9 Monitor

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. It is important to record any relevant information about specific changes to hardware, software, or firmware such as version or release numbers, descriptions of new or modified

features/capabilities, and security implementation guidance. It is also important to record any changes to the environment of operation for the information system (e.g., modifications to hosting networks and facilities, mission/business use of the system, threats), or changes to the organizational risk management strategy. The information system owner and common control provider use this information in assessing the potential security impact of the changes.

Documenting proposed or actual changes to an information system or its environment of operation and subsequently assessing the potential impact those changes may have on the security state of the system or the organization is an important aspect of security control monitoring and maintaining the security authorization over time. Information system changes are generally not undertaken prior to assessing the security impact of such changes.

6.9.1 Annual Assessment

Annual Assessments are required as part of OMB circular A-130. In general, at least one third of the security controls must be assessed annually to ensure they are implemented correctly and operating as intended. Contingency plans must also be reviewed and updated and tested as part of this annual assessment. The one third requirement of testing security controls is not required for OA systems, which are required to maintain their security posture on a continuous basis.

OA systems are required to create a CAT to determine security control testing frequencies based on a risk assessment of each control.

The CP must be reviewed and tested at least annually. It should reflect the current state of the system procedures to bring the information system back up to full operating capacity from a disrupted state. The CP test should be conducted commiserate with the impact of the availability security objective (low availability system requires a call tree exercise; moderate availability system requires a tabletop exercise; high availability system requires a full functional exercise).

Once the CP and CPT are conducted as part of the annual assessment, the DR team receives notification. The DR team will then conduct a review in accordance with the DR checklist and either approve or reject the CP and CPT.

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."

Controls required to be assessed annually for CFO-designated Systems are located in Attachment R, "Compliance Framework for CFO-designated Financial Systems" to the *DHS 4300A Sensitive Systems Handbook*. Attachment R is limited to the controls that are reviewed annually (and does not contain the requirements of OMB Circular 123). This includes updating the security control assessment and SAR annually.

In addition, the DHS CISO tri-fold identifies the NIST Special Publication (SP) 800-53 controls that have been designated for CFO systems but does not include the relevant controls from the *DHS Sensitive Systems Handbook*.

7.0 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 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.

DHS implements OA in three layers, which collectively ensure constant control assurance:

- Layer 1: Common and Inherited Controls and Reciprocity
- Layer 2: Continuous Monitoring
- Layer 3: Event-Driven Monitoring

Event-Driven Monitoring (Layer 3) involves evaluating and testing controls when security events or "triggers" occur that may have an impact on the system's security status. Following an event, a review is conducted to determine the impact on the status of controls and risk to the system. Some key process highlights include the following:

- An Operational Risk Management Board (ORMB), composed of various subject matter experts, evaluates security triggers and makes risk-based recommendations.
- Following ORMB review, the CISO prepares a formal recommendation to the Authorization Official (AO) about whether or not to maintain the authorization.

Security triggers are to be entered into IACS as Risk Elements.

FISMA systems entering into the OA program must meet the below eligibility criteria and submit a formal application to participate in the DHS OA program. Criteria for eligibility includes but is not limited to:

- ISCM Metrics are reported for each system.
- Weakness Remediation Metrics in good standing
- Systems providing common controls are properly provisioned in IACS to provide control inheritance.
- Chartered Organizational Risk Management Board in place
- Designated Ongoing Authorization Manager assigned
- Approved Privacy Compliance exists

- ATO Expiration should be greater than 60 Days of OA Entry submission
- No major changes (platform upgrades, physical and environmental changes, modernization efforts, etc.) to the system occurred since the last granted ATO

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.

In general, once a system has been approved for OA, all updates to the system documentation should be done under Task 6 in the current SA tool workflow. 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."

OA requirements are documented in the DHS OA Methodology. Components will refer to the OA Methodology prior to submitting any systems for entry into the OA program.

For more information about ongoing authorization, please refer to the Ongoing Authorization Methodology guide.

Figure 4: OA Relationship to RMF

8.0 CLOUD AND FEDRAMP AUTHORIZATIONS

8.1 Introduction to Cloud

Cloud computing relies on restricting sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. Cloud computing provides scalable information technology (IT) capabilities that are offered as a service over the Internet to many users at one time. Multiple agencies can share pooled IT resources, such as an email service, that reduce costs and improve efficiency.

8.2 Clouds Categorized by Deployment Models

The deployment model is based on the organizational structure, provisioning location, security considerations, and budget. The cloud deployment models are:

- A "public" cloud infrastructure is available to the general public and is owned by a third party cloud service provider (CSP). In a public cloud, an agency dynamically provisions computing resources over the Internet from a CSP who shares its resources with other organizations. Similar to that of an electric utility billing system, the CSP bills the agency for its share of resources. This can be the most cost effective deployment model for agencies as it gives them the flexibility to procure only the computing resources they need and delivers all services with consistent availability, resiliency, security, and manageability. Nevertheless, to benefit from a public cloud, an agency must accept the reduced control and monitoring over the CSP's governance and security.

- A "private" cloud infrastructure is operated solely for a single organization or agency: the CSP dedicates specific cloud services to that agency and no other clients. The agency specifies, architects, and controls a pool of computing resources that the CSP delivers as a standardized set of services. A common reason for agencies to procure private clouds is their ability to enforce their own data security standards and controls. An agency will typically host a private cloud on premises, connect to it through private network links, and only share its resources within the agency. Because resources are not pooled across multiple unaffiliated organizations, an agency will pay for all of the cloud's capacity. Nevertheless, the agency's Chief Information Officer (CIO) can provide these resources as services on-demand to organizations and programs within the agency and charge them accordingly.
- A "hybrid" cloud comprises two or more clouds (private, community, or public) with a mix of both internally and externally hosted services. Agencies will likely not limit themselves to one cloud deployment but will rather incorporate different and overlapping cloud services to meet their unique requirements. Hybrid deployment models are complex and require careful planning to execute and manage especially when communication between two different cloud deployments is necessary.

8.3 FedRAMP Introduction

The Federal Risk and Authorization Management Program (FedRAMP) provides a cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies:

- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels;
- A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by Cloud Service Providers (CSPs);
- Authorization packages of cloud services reviewed by a Joint Authorization Board (JAB) consisting of security experts from the Department of Homeland Security (DHS), Department of Defense (DOD), and General Services Administration (GSA);
- Standardized contract language to help Executive departments and agencies integrate FedRAMP requirements and best practices into acquisition; and
- A repository of authorization packages for cloud services that can be leveraged government-wide.

8.4 FedRAMP JAB and Agency Authorizations:

FedRAMP processes are designed to assist agencies in meeting FISMA requirements for cloud systems and addresses complexities of cloud systems that create unique challenges for complying with FISMA.

There are three paths for security packages to make their way into the FedRAMP repository. Once a security package is listed in the FedRAMP repository, federal agencies then have the opportunity to review the packages to determine if they would like to use the system described in the package. Some of the packages listed in the repository are either approved or in the process of review for approval by FedRAMP.

8.4.1 FedRAMP JAB Authorization:

FedRAMP candidates must prepare for the review process by going through a readiness review, conducted by the PMO. CSPs that pass the readiness review are placed in the queue for a FedRAMP kickoff. The kickoff meeting will go through all of the documentation and the readiness review information, which includes a number of control checks as a way to ensure that the CSP has met a level of readiness for the 90 day review and assessment period. The 90 day review includes an assessment by the chosen PMO certified Third Party Assessment Organization or 3PAO of all of the controls required for the FISMA Security Impact Category of the system, as well as all of the documentation required to be submitted. Once complete, the JAB will determine if the P-ATO should be granted. CSPs that require changes that exceed the 90 day review period will need to restart the review process after the required changes are implemented.

8.4.2 FedRAMP Agency Authorizations:

For Agency ATO, the systems have to go through the regular DHS security authorization process and also have to implement the FedRAMP security controls based on the FISMA security impact category controls. However, because the agency is accepting the risk for their system, if a control impacts the mission and the system owner is willing to accept the risk for that control not being implemented, they may create a waiver and/or POA&M for that control. In accordance with DHS 4300A policy, all security authorizations are conducted and recorded in the Information Assurance and Compliance System (IACS). FedRAMP systems are implemented, assessed, and monitored in IACS like any normal system. IACS uses control inheritance to leverage a FedRAMP system. In order to use a FedRAMP system, the Common Control Team (CCT) must be informed. To submit a request to the CCT, please contact the DHS Information Security Customer Service Center (Infosec Helpdesk). After obtaining access, leveraging a FedRAMP system is similar to inheriting controls from a non-FedRAMP system. Refer to the DHS Common Controls Implementation Guide v2.2 for guidance.

8.4.3 Leveraging existing FedRAMP ATO, both Agency and JAB:

It is possible to leverage an existing ATO from a CSP or service which already has a FedRAMP ATO. For Agency ATOs, the consumer will need to do a risk assessment to determine if the risk accepted by the owner of the agency ATO is the same as the consumer's. If the risk differs, the consumer will need to apply for their own Agency ATO.

8.4.4 Once the FedRAMP ATO is granted:

Within the FedRAMP Security Assessment Framework, once an authorization has been granted, the CSP's security posture is monitored using JAB/Agency approved tools according to the assessment and authorization process. Monitoring security controls is part of the overall risk management framework for information security and is a requirement for CSPs to maintain a security authorization that meets the FedRAMP requirements.

Traditionally, this process has been referred to as "Continuous Monitoring" as noted in NIST SP 800-137 *Information Security Continuous Monitoring for Federal Information Systems and Organizations*. Other NIST documents such as NIST SP 800-37, Revision 1 refer to "ongoing

assessment of security controls". It is important to note that both the terms "Continuous Monitoring" and "Ongoing Security Assessments" mean essentially the same thing and should be interpreted as such.

As described in the FedRAMP requirements, CSPs must provide monthly reports of all vulnerability scanning to authorizing officials for review and tracking these vulnerabilities within the POA&Ms. These deliverables are really a subset of the evidence required at time of authorization. In this vein, the analysis of these scan results should be performed in the same manner they were for time of authorization. In particular, this means:

- All scan findings must be documented (including low findings).
- Each unique vulnerability is tracked as an individual POA&M item.
- Deviation requests must be submitted for any requested changes to scan findings (e.g. risk adjustments, false positives, and operational requirements).

On a monthly basis, Authorizing Officials will be monitoring these deliverables to ensure that the CSP maintains an appropriate risk posture – which typically means the risk posture stays at the level of authorization or improves. As a part of any authorization letter, CSPs are required to maintain a continuous monitoring program. CSPs should understand that this means their continuous monitoring deliverables and associated view of risk posture means that this analysis on a monthly basis leads to a continuous authorization decision every month by Authorizing Officials.

For FedRAMP specific references, refer to Appendix E.

APPENDIX A – DOCUMENT REVIEW METHODOLOGY

1.0 INTRODUCTION

This methodology was developed by the Department of Homeland Security (DHS) Federal Information Security Modernization Act (FISMA) Cybersecurity Risk Management and Compliance (CRMC) Division of the DHS Chief Information Security Office (CISO) to ensure that DHS Security Authorization (SA) Document Reviews (DR), for Sensitive But Unclassified (SBU) systems, are of high quality and are conducted in a timely manner.

1.1 Purpose

This document serves as a guide for internal CISO DR Team members and for DHS Component compliance personnel regarding how the DR process is conducted and describes the roles and responsibilities of each stakeholder in the process.

1.2 Scope

This document only addresses reviews of DHS Sensitive But Unclassified (SBU) systems. Document reviews for National Security Systems (NSS) are conducted by the Intelligence and Analysis (I&A) division. The document review process for NSS should be found on the NSS SharePoint site.

1.3 Audience

This document is intended for CISO DR Team members and for DHS Component compliance personnel.

2.0 BACKGROUND

Under the authority of the DHS Chief Information Officer (CIO), the CISO is the primary authority for ensuring compliance with the Federal Information Security Modernization Act (FISMA) of 2014, National Institute of Standards and Technology (NIST) guidance, Office of Management and Budget (OMB) circulars, and all applicable laws, directives, policies, and directed actions on a continuing basis.

Per Section 2.1.2 of DHS Directive 4300A Sensitive Systems Handbook, the CISO "Reviews and approves the tools, techniques, and methodologies planned for use in certifying and authorizing DHS systems, and for reporting and managing systems-level FISMA data. This responsibility includes reviews and approval of Security Control Assessment plans, Contingency Plans, and security risk assessments..."

2.1 Goals of CISO DR Team

The goals of the CISO DR Team are to:

- Validate that a minimum set of quality standards as expressed in the DHS DR Checklist have been implemented across all DHS SA packages
- Ensure that applicable DHS and NIST controls are properly documented

- Ensure that SCA results are consistent with a valid Component risk assessment process
- The CISO DR Team ensures that SBU SA documents are in compliance with DHS Directive 4300A Sensitive Systems Policy, and applicable NIST and OMB guidance

2.2 Objectives of the CISO DR Team

The CISO DR Team's objectives are to:

- Assess the completeness of the information provided in SA documentation against DHS quality standards.
- Provide feedback to refine the SA process and identify trends across Component packages to determine the root causes of deficiencies.

3.0 SECURITY AUTHORIZATION VALIDATION PROCESS

The Security Authorization process is vital to verifying a system's security posture. Through comprehensive system document reviews, DHS CISO reviewers ensure that Department Systems are compliant with FISMA requirements, meet NIST and DHS control implementation standards, and are eligible for initial and continued operation. The Department adheres to a maximum three-year authorization cycle policy, requiring that systems re-submit system documentation to CISO every three years, or when a significant change occurs, to obtain or maintain a valid Authorization. This review process is called the Document Review process.

The OCISO Document Review Team reviews artifacts submitted as part of the SA package against a document review checklist. The primary objective of the Document Review process is to ensure completeness and consistency with applicable laws, regulations, directives, and guidance.

Step	Task	Responsible Party	Result
1	Complete RMF Tasks 1-5 in IACS	System personnel	Activates Component Document Review in IACS.
2	Complete Component Document Review	Component ISSM	Activates DHS Document Review in IACS.
3	Conduct DHS Document Review	DHS Document Review Team	Pass – DHS Document Review approves the task in IACS. Go to step 4 or; Fail – DHS Document Review Team notifies Component ISSM that documentation requires updates. Go back to step 1.
4	Complete Authorization Decision Task in IACS	Component ISSM	Updates the ATO expiration date.

3.1 Document Review Methodology

The DHS Document Review Methodology is organized into four stages

(5) Initiation via the IACS Task Notification outlines the process for initiating the DR process for the IACS.

(6) Document Review outlines the process(s) for conducting reviews whenever a notification is received.

(7) Results details the criteria used by the CISO DR Team to issue a decision regarding the Checklist after a package has been reviewed and to tailor future training sessions to continually improve Component document quality.

(8) Completion via IACS Task Notification stage outlines the process for completing the DR process through IACS.

3.2 Initiation via the IACS Task Notification

To initiate a package review, the system Information Security System Manager (ISSM) will complete Tasks 1 through 5 (Component Document Review) of the IACS workflow. When the component approves the Component Document Review task, IACS automatically sends an alert to the Certification and Accreditation mailbox (canda@HQ.DHS.GOV) alerting the CISO DR Team it can conduct its review.

Additionally, the CISO DR Team receives alerts for the following types of reviews:

- DHS Document Review (a full package review)
- Annual Contingency Plan (CP) Review
- Annual Contingency Plan Test (CPT) Review
- Annual CFO Control Review

3.3 Package Categories

Due to the workflow process, which is the core of the IACS, Security Authorization packages can only be reviewed, approved, or rejected as an entire package.

The standard SA documents reviewed by the CISO DR Team include the following:

- Contingency Plan
- Contingency Plan Test
- Security Assessment Plan
- Security Assessment Report
- Security Plan

As needed, the CISO DR Team may also review additional documents to support the security authorization process:

- Interconnection Security Agreement (ISA)
- Memorandum of Understanding (MOU)
- Configuration Management Plan (CMP)
- Information System Security Officer (ISSO) Letter
- Alternate Information System Security Officer (AISSO) Letter

- Plan of Action and Milestones (POA&M)
- Risk Assessment (RA)
- Transmittal Letter

System personnel should upload supporting documentation, such as relevant policy documents, Standard Operating Procedures (SOPs), waivers, memoranda of agreements (MOAs), and service level agreements (SLAs) into the "General Information" section of IACS. All IACS tasks with extensible documents must be updated and recently published.

3.4 Document Review Checklists

The DR checklist ensures that the Security Authorization Package is complete. The checklist correlates to the FIPS 199 rating of the system, and provides the applicable baseline controls for confidentiality, integrity, and availability.

For each document without a dedicated checklist, a minimum set of criteria is evaluated as follows:

- Consistency – The information stated in the document must be consistent across the entire package.
- Identification – All documents must identify with the appropriate system and system-relevant information.
- Complete fields – All relevant and required fields of information must be completed.
- Electronic approval of the IACS – When required, signature from the appropriate authorities must be present.
- **Date –** Documents must fall within the cycle of authorization in which the system is renewing or initiating. Upon receiving IACS notification of documents to review, the CISO DR Team reviews the documents against the DR Checklist. Each document will be assessed with one of the following conditions:
  - **Pass (P) –** All significant document requirements are satisfied
  - **Pass with comments (PC) –** The document requirements are addressed, but require clarifying information.
  - **Fail (F)** – Significant document requirements are missing and/or are inaccurate.

Packages are reviewed in the order they are received (i.e. first in/first out). The CISO DR Team's goals are to review and respond to CP and CPT reviews within two working days of receipt, and full package reviews within seven working days of receipt. However, these timeframes are affected (and may be delayed) by the number of DR actions within the team's queue at any given time. Components should submit actions for DHS DR review 30 days prior to any ATO or document expiration to allow for review and any required corrections to documentation.

3.4.1 Security Plan

Each control response is evaluated for clarity, brevity, completeness, and correctness with regards to four criteria:

(1) What is the solution? The solution can be a device, document, process, or plan. It must be clearly stated as the object that governs the implementation of the security control.

(2) How does the solution satisfy the control or requirement? The solution being discussed must be directly correlated to the presented requirements. It must be clear to the reviewer how the system uses the solution for each system layer (i.e.; Operating System, application, database, and Web, if applicable) to satisfy the requirements established by that particular security control.

(3) Who is the responsible party for solution management? Although the ISSO may be responsible for the oversight of system security measures, a system-specific role should also be identified as managing, operating, or implementing control- relevant security measures.

(4) How frequently is the solution updated or reassessed? Control solutions may be initiated once and continually monitored or they may require continual implementation (as the case with revisions or updates) or a combination of the two. The timing of the solution implementation should be addressed for each requirement. Note: A specific timeframe must be provided (e.g., quarterly, monthly, or every eight weeks); a timeframe of "periodically" is not sufficient.

Section I of the SP contains information on the system environment, purpose, characteristics, accreditation boundary, and technologies employed of the system. Section I must receive a 100% pass rate in order for the review to continue; otherwise, it will be returned to the Component POC to be updated.

Section II of the SP is evaluated by randomly selecting three NIST SP 800-53 control families. Section II must receive a minimum of 90% in order for the entire SP to pass. For example, if the initial review of Section I yields a 100% passing rate and Section II yields a 90% or above passing rate; the entire SP passes. If the passing rate of those three control families are less than 90%, the SP fails and the security authorization package will be reactivated in IACS for review and resubmittal. Note: All 4300A Attachment R Controls will be reviewed for CFO-designated systems. Controls will be assessed with the following conditions:

- **Pass (P)**: DHS security control implementation criteria is satisfied.
- **Pass with comments (PC)**: Implementation criteria is satisfied; however, additional detail is needed for a more complete response. The reviewer will specify the additional information required.
- **Fail (F)**: Criteria is missing, does not explain system-specific implementation, provides inaccurate information and/or remediation/mitigation plans are missing.
- **Not Applicable (N/A)**: The control does not apply based on system categorization and/or accreditation boundary

When corrections are made and all of the approvals are completed, Component Document Review Task in IACS. IACS will automatically send notification to the "C and A" Mailbox (canda@HQ.DHS.GOV) alerting the CISO DR Team when the package is reapproved

3.4.1.1 Documenting Implemented (tiered) Controls

Systems are required to document controls to describe each element of its implementation. Figure 5 shows an example of a control implementation for SI-2 as found in Section II of the SP that has passed DHS DR review. Additionally, this control's implementation section illustrates

how the solution for each layer of the control (i.e., OS, application and database) is described separately.

Flaw Remediation						SI-2
Requirement The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process.						
Implemented [X]	Not Implemented [ ]	Planned [ ]	Inherited [ ]	Partially Inherited [ ]	Compensated [ ]	N/A [ ]
Implementation: (a) *System X* identifies system **OS** flaws through monthly scanning of system devices by the SOC using Tenable Nessus and stores the scan reports on a database server that is accessed by the ISSO via the SARGE utility tool. System Flaws are corrected by submitting proposed patches, service packs, hot fixes and updates to the CCB for approval using REMEDY. (b) System *X* identifies system **application ABC's** flaws (if applicable) through monthly scanning of system devices by the SOC using (Tenable, vendor updates, etc.) … System *X* identifies system **database** flaws (if applicable) through monthly scanning of system devices by the SOC using DB Protect… (c) *System X* requires lab testing prior to controlled change release unless immediate risk requires immediate intervention. All impacted sites will be compliant within 90 days of change release. (d) *System X* incorporates flaw remediation into the organizational CM process by submitting all patches, service packs, hot fixes and updates to the CCB for approval unless there is an immediate risk requiring immediate intervention. Responsibility: The ISSO is responsible for reviewing this control at least annually or when there is a change to the Information System.						

Figure 5: Implemented Control Response

Note: Depending on the control implemented (e.g., certain Program Management or Training controls) layered implementation statements may not be required.

3.4.1.2 Documenting Planned Controls

POA&Ms must be referenced whenever a security control implementation status is "Planned." Figure 6 shows an example of a planned control implementation for MP-6 as found in Section II of the SP that has passed DHS DR review.

Media Sanitization						MP-6
Requirement The organization: a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.						
Implemented [ ]	Not Implemented [ ]	Planned [X]	Inherited [ ]	Partially Inherited [ ]	Compensated [ ]	N/A [ ]
Implementation: System X currently does not have a documented procedure for sanitizing information system media, digital nor non-digital, prior to disposal, release out of organizational control, or release for reuse. System X is currently drafting procedures to address this control and plans to have these procedures approved within 6 months. See POA&M # 25. System X currently does not have a documented procedure for employing sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information. System X is currently drafting procedures to address this control and plans to have these procedures approved within 6 months. See POA&M # 25. Responsibility: The ISSO is responsible for reviewing this control at least annually or when there is a change to the Information System.						

Figure 6: Planned Control Response

Planned or Not Implemented controls require identification of both compensating measures and supporting POA&Ms. When reviewing controls that are planned or not implemented, the CISO DR Team will review the POA&M(s) listed in IACS to verify the following information:

- The POA&M number in IACS matches the POA&M number listed in the SP.
- The POA&M recorded in IACS actually addresses the control in the system's SP.

3.4.2 Contingency Plan and Contingency Plan Test

The CP and CPT can only be properly developed after a business impact analysis (BIA) has been conducted for the system. Although the CISO DR Team does not review the BIA, it is an essential component of contingency planning.

The CP must outline the type of scenario to which it is meant to respond and give details on how it integrates with other, larger organizational plans such as disaster recovery plans or continuity of operations plans. Additionally, the CP must outline restoration procedures, identify teams and personnel involved at each stage of restoration, and define restoration objectives for each team. If SLA, MOU, or MOA are in place, they must also be referenced and discussed.

The CPT focuses on testing the plan(s) established by the CP. The level of testing (i.e. type of exercise conducted) is dependent upon the availability level of the system. Separate checklists and templates exist for each of the three availability levels. If the appropriate level of testing as required by DHS 4300A cannot be conducted (e.g. a full functional exercise), the CPT must provide a reason why and have a waiver submitted.

The CPT must simulate a response to an unanticipated event. Documenting how major changes/upgrades to a system are to be conducted (or were conducted) does not count as a valid test of the contingency plan.

Note: Please refer to DHS Sensitive Systems Policy Directive 4300A, element 3.8.b, for defining a major change/ upgrade as "major modifications that have the potential to significantly impact risk are made to sensitive information systems, or to their physical environments, interfaces, or user community."

3.4.2 Security Assessment Plan

The SAP is evaluated to understand how the Component plans to conduct its testing of security controls as well as to check the hardware, software, operating systems, network interfaces, and access methods are all documented and tested. Any system components excluded from testing must be identified separately, and the SAP must also document all testing tools and testing methods.

3.4.3 Security Assessment Results

The Security Assessment Report (SAR) is evaluated to ensure test results are provided for each control and the appropriate mitigation steps are being implemented such as opening POA&Ms; or submitting requests for risk acceptance and/or waivers. Risk acceptance can be approved by the AO for NIST controls. Waivers must be approved by the DHS CISO.

3.4.4 Requirements Traceability Matrix (RTM)

The RTM ensures that all security requirements are identified and investigated. Each row of the matrix identifies a specific security requirement and provides the details of how it was tested and/analyzed.

3.5 Segregation of Duties

DHS 4300A 4.1.4 states "Segregation of duties is intended to prevent a single individual from being able to disrupt or corrupt a critical security process." The IACS workflow implements this policy by requiring multiple approvals (ISSO, ISSM, DHS DR) for key security documents.

Tasks in IACS that have been approved at the component level by the same individual will not be approved by the CISO DR Team unless:

- The designated ISSM is approving in lieu of the ISSO
- The designated ISSM is approving in lieu of the SCA - Security Control Assessor (for Low impact systems)
- The component has a DHS CISO approved waiver allowing the ISSO, (or alternate ISSO) to approve on behalf of the ISSM.

Components that have personnel resource limitations that necessitate the need for select individuals to perform multiple roles in IACS must obtain a waiver from DHS CISO before individuals will be granted multiple roles in IACS.

4.0 REVIEW RESULTS

If all documents pass review, the CISO DR Team will approve the "DHS Document Review" task in IACS and upload the DHS DR checklist into "Managed Project Artifacts." IACS will automatically send an approval notification to the ISSO, Alternate ISSO, and Component CISO/designee.

If one or more documents fail review, the DR Team will disapprove the DR action and contact the component representative using one of the methods described below.

- Annual CP/CPT Reviews: The DR Team will reject the package in IACS and provide an e-mail to the component POC as to why the security package failed document review.
- DHS DR Task (Full Package Review) – The CISO DR Team will contact the component POC and request that the task be recalled for corrections. Failure to recall the task within 24 hours will result in the DR Team reactivating the Component Document Review Task in IACS. This process will be replaced when IACS is updated to provide a "reject" option for the full package.

4.1 Conference Calls

At the completion of a review, a conference call may be requested by the Component to discuss any deficiencies in documentation and to assist the Component with understanding any controls that did not pass. Conference calls are intended to help improve the long-term quality of the Security Authorization process and prevent recurring documentation issues. CRMC will not initiate conference calls.

4.2 Re-reviews

A second document review is necessary only if the Component package failed its initial review. Documents are only assessed for those line items that failed the initial review.

Please note that all changes to the new document(s) will be cross-referenced for consistency throughout the package. If changes are inconsistent with other supporting system documentation, then the documents will "**Fail**." *Additionally, Component packages must have a completed security plan. A security plan must address at least 90 percent of their security controls to be considered complete.* If 90 percent of the security controls are not addressed the Security Authorization Package will "**Fail."**

4.3 DR Process completion

Upon CISO DR Team approval of the DHS DR task, an IACS-Alert is automatically sent to the AO and ISSM mailbox indicating that the component can complete the Authorization Decision Task.

AOs may issue an ATO for a period of up to three years. AOs may choose to issue an ATO for a period of less than three years; however, any subsequent ATOs issued within the three year period must be supported by a re-completion of Task 4 in IACS.

5.0 EDUCATION AND OUTREACH

The CISO DR Team is a resource to all Components during the development of their SA packages for guidance and clarification. The CISO DR Team develops, tailors, and delivers external education sessions through the compilation of feedback received by ISSM/CISO correspondence, ISSOs, document developers, Component FISMA teams, and previous training sessions.

The CISO DR Team identifies trends across Component packages that may signify a lack of requirements or process understanding; this information is important when recommending

changes to Departmental policies or procedures. The team also seeks to improve feedback and communication between Components and DHS HQ by conveying expectations and support. Our training team is available to perform initial or refresher training on how Document Review is performed. For requests for DR training, please contact ISOtraining@hq.dhs.gov.

APPENDIX B – AUTHORITY TO PROCEED

1.0 INTRODUCTION

The DHS OCISO Authority to Proceed (ATP) process is specific to new DHS information systems pursuing an agile development methodology and residing on infrastructures that have a DHS Authorization to Operate (ATO) concurred by the DHS CISO or a user of a FedRAMP approved ATO. The process in this guide allows Federal Information Processing Standards (FIPS) Publication (PUB) 199, *"Standards for Security Categorization of Federal Information and Information Systems"* Low and Moderate impact systems to be granted ATPs for one (1) year after completing the tailored NIST RMF processes detailed in this guide.

The ATP process is designed for systems that can prove they are built securely through a limited security assessment. The purpose of this process is to ensure cybersecurity risk is managed while shifting the focus of the assessment to mission performance in an operationally relevant environment versus control documentation.

The ATP process:

- Allows components to assess limited set of security controls (baseline controls) in order to demonstrate secure resiliency.
- Covers at a minimum, the five NIST Cybersecurity Framework function areas (Identify, Protect, Detect, Respond and Recover) in the minimal security control baseline.
- Allows additional security controls to be tested by the Components in addition to the minimum required baseline controls.
- Provides Components one (1) year to implement remaining controls and obtain an ATO.
- Scores system on the FISMA Scorecard immediately upon being granted an ATP.
- Ensures predefined eligibility criteria is met by the Components

DHS CISO has developed this process with certain guidelines:

- This process is primarily designed to authorize new systems or new acquisitions, under the paradigm that new systems use industry best practice SELC processes that incorporate cybersecurity.
- DHS CISO would consider Software as a Service (SaaS) products or applications designated for cloud migration to be appropriate candidates assuming that the underlying infrastructure is already accredited with appropriate security safeguards and countermeasures are in place, i.e. FedRAMP approved Infrastructure as a Service (IaaS) or Platform as a Service (PaaS).
- Systems should operate in a FedRAMP authorized on premise or cloud environment to ensure proper defense-in-depth safeguards and countermeasures are in place.
- The Information System Owner and their staff have implemented a viable and effective system level continuous monitoring strategy that uses automated scanning tools.
- This process is not designed for systems that anticipate providing their ATO package to requesting organizations under reciprocity, due to concerns with requesting AO acceptance of minimal documentation compared to traditional requirements.

- This process is not designed for enclave accreditations, due to the necessity of enclaves to provide inheritable controls for systems operating within the enclave.

Any system following the ATP process will have a higher risk than a system following the traditional ATO process. For this reason, all systems following this process must be approved for the ATP process by both component and DHS CISOs during the initiation phase of the system's lifecycle. For this reason, the following system types are not permitted in the ATP process:

- CFO-designated Systems
- Privacy Sensitive Systems
- High-Value Asset (HVA)/Mission Essential Systems (MES)
- Publicly Accessible Systems
- External Information Systems

Note: This process will follow a phased approach. Additional guidance on FedRAMP Systems, Privacy Sensitive Systems, CFO-designated systems, HVA/MES systems, etc. will be provided.

2.0 ATP ENTRY PROCESS

As a requirement of the ATP Process, DHS AO/CISO will grant the system team one (1) year to have the ATO requirements completed. The following eligibility criteria has to be met by the Component prior to submitting it to DHS CISO:

- System is a new system in initiation
- System is not a Privacy Sensitive System
- System is not a CFO-designated System
- System is not a HVA/MES System
- System is not an External facing system
- System is not an External Information System
- System does not have a 'High' Security Categorization (FIPS199)
- If system is hosted in the Cloud, the CSP should be FedRAMP authorized.
- Completion of the following documentation:
  - FIPS199
  - PTA
  - E-Authentication
  - BIA (Although DHS CISO Office does not review the BIA, it is an essential component of contingency planning and helps determine the Availability of the System for the Security Categorization of the system)

Once the above conditions have been met, the Component completes and signs the DHS ATP Entry Letter Template along with the list of additional security controls that they will assess as part of the limited SCA and submits it to the DHS FISMA Inventory Mailbox

(FISMA.Inventory@HQ.DHS.GOV) for processing. The ATP Entry Letter is then reviewed and approved by the DHS CISO and the ATP Control Overlays are initiated in IACS for the System.

3.0 BASELINE CONTROLS

The DHS CISO has published the minimally required control list (Table 1 below) and will update it regularly. Each Component CISO has the ability to add to the control list as necessary. The limited assessment of security controls will greatly reduce the workload and will allow the system to become operational quicker than the traditional process for receiving an Authority to Operate (ATO). Once the controls have been implemented and assessed, the Component Authorizing Official may grant an ATP with the DHS CISO's agreement, provided that the limited assessment does not have an overall high risk level.

4.0 ATP PROCESS

The ATP process demonstrates security in the following manner and includes the following steps:

- Security Baseline: Program Managers (PM) and System Owners must implement a limited security baseline that covers NIST Cybersecurity Framework function areas and categories that are required to report on for the Federal Information Security Modernization Act (FISMA). This includes the required security controls in Table 1 as well as any additional controls that the Components choose to assess.
- Completion of limited documentation (Security Plan) (Note: The Limited documentation includes the partially completed security plan which includes Section 1 of the Security Plan and documented baseline controls as well as any additional controls selected.)
- Limited security assessment: To receive an ATP for the system a subset of predefined critical controls (baseline controls) shall be implemented and assessed. This is a change from how the Authority to Operate (ATO) was done where the assessment was focused on the entire control baseline from the National Institute of Standards and Technology (NIST) Special Publication 800-53.
- Weakness Remediation: POA&Ms need to be managed and tracked in IACS for all findings. Remediation of all high findings should be completed prior to ATP approval (this includes the vulnerability scan results as well).
- Approval of ATP Memo by the Component AO (that also includes the SAR, Remediation Plan and Signed ATP Entry Letter). The Component submits and uploads the Signed ATP Memo to DHS CISO Office through IACS under the 'Component Documents Review' task for approval.

5.0 SAR/SAP VERBIAGE

The following ATP verbiage needs to be included in the Limited SAR/SAP by Components:

> "Assumption: This is a limited Security Control Assessment that is being conducted on a selected set of controls approved by DHS CISO as well as any

additional controls that the Component's deem fit. The assessors will only assess these controls for this limited assessment in addition to any vulnerability scans and any documentation available for the controls."

**Note: The Limited documentation includes the partially completed security plan which includes Section 1 of the Security Plan and documented baseline controls as well as any additional controls selected by the Component.*

6.0 POST ATP APPROVAL

After ATP is granted, the system will move into the SELC *Implementation* phase and become reportable on the Federal Information Security Management Act (FISMA) Scorecard. It can also initiate processing of production data. One year from the time the ATP is issued, all remaining security control documentation and a full assessment must be completed as required by the ATO process. As part of the ATO process, all the security controls will be tested including the ones already tested during the ATP limited assessment. The Components can leverage some of the ATP artifacts and documentation for the ATO process. Any failed controls from the ATP assessment will be assessed in depth by the assessors along with appropriate weakness remediation and POA&Ms. If an ATO is not received within one year of the ATP, the system will become non-compliant and the ATP will be revoked, thereby affecting the FISMA Scorecard.

Systems approved for ATP will not be allowed to move into the Ongoing Authorization Program unless a full assessment has been completed and an ATO is granted.

Continuous monitoring is a key step in determining the security posture of the system. This may include but not be limited to vulnerability scans, audit logging tools, patch management, etc. The overall security posture will be determined once the tools have been configured and the system is being reported on the FISMA Scorecard.

7.0 ATP PROCESS WORKFLOW

The steps below provide the overall workflow steps on the ATP Process.

7.1 ATP Entry Letter Initiation Steps

- The Component submits the ATP Process Entry Letter signed by the Component CISO, to DHS CISO Office via DHS FISMA Inventory Mailbox.
- The Inventory Team reviews the checklist and verifies the Component has met the requirements.
- FISMA Inventory Team sends the ATP Process Entry Letter to DHS CISO/Designee for signature.

7.2 ATP Entry Workflow Initiation Steps

- The Inventory Team will apply the ATP overlays for the 'Moderate' or 'Low' security baseline systems in IACS under 'Inventory/OMB Requirements' task.

- The DHS Inventory Team notifies the Component through email of their acceptance into the ATP workflow process and the ATP Entry letter will be uploaded as an artifact in IACS.
- The Component will work on the following:
  a. Additional controls selected by the Component will need to be tailored in by the System ISSO.
  b. Security Plan updates for the baseline controls and any additional controls being tested.
  c. The Security Assessment Report should not have any High findings (this includes the vulnerability scan results).
- Once the Limited Assessment has been completed, the Component follows the current IACS process to submit and upload the ATP Memo signed by the Component AO under the 'Component Documents Review' task for DHS CISO approval.
- The DHS Document Review team conducts the review and approves the 'DHS Document Review' task in IACS.
- The Component AO approves and grants the ATP under the 'Authorization Decision' task in IACS.
- Once the 'Authorization Decision' task in IACS is approved, an update to the Inventory CR form needs to be submitted within 30 days of the ATP being granted along with the Signed ATP Memo to change the SELC status to 'Implementation' (which will show up on the scorecard). In addition, the Inventory Team removes the selected ATP overlay in order to return to the full control baseline. (Note: ATP date on the Inventory CR Form is the Date the ATP Memo was signed by the Component AO)
- The Component has a period of 1 year from the ATP Date to accomplish the remaining ATO requirements else the ATP will expire.

7.3 ATO Completion Steps

- Another update to the Inventory CR form will be submitted by the Component once the ATO is approved to update the ATO Date and SELC status to 'Operational'; and change the status from ATP to ATO in the FISMA Inventory Database and IACS.

Note: In order to accommodate the ATP process, the IACS workflow will be slightly modified.

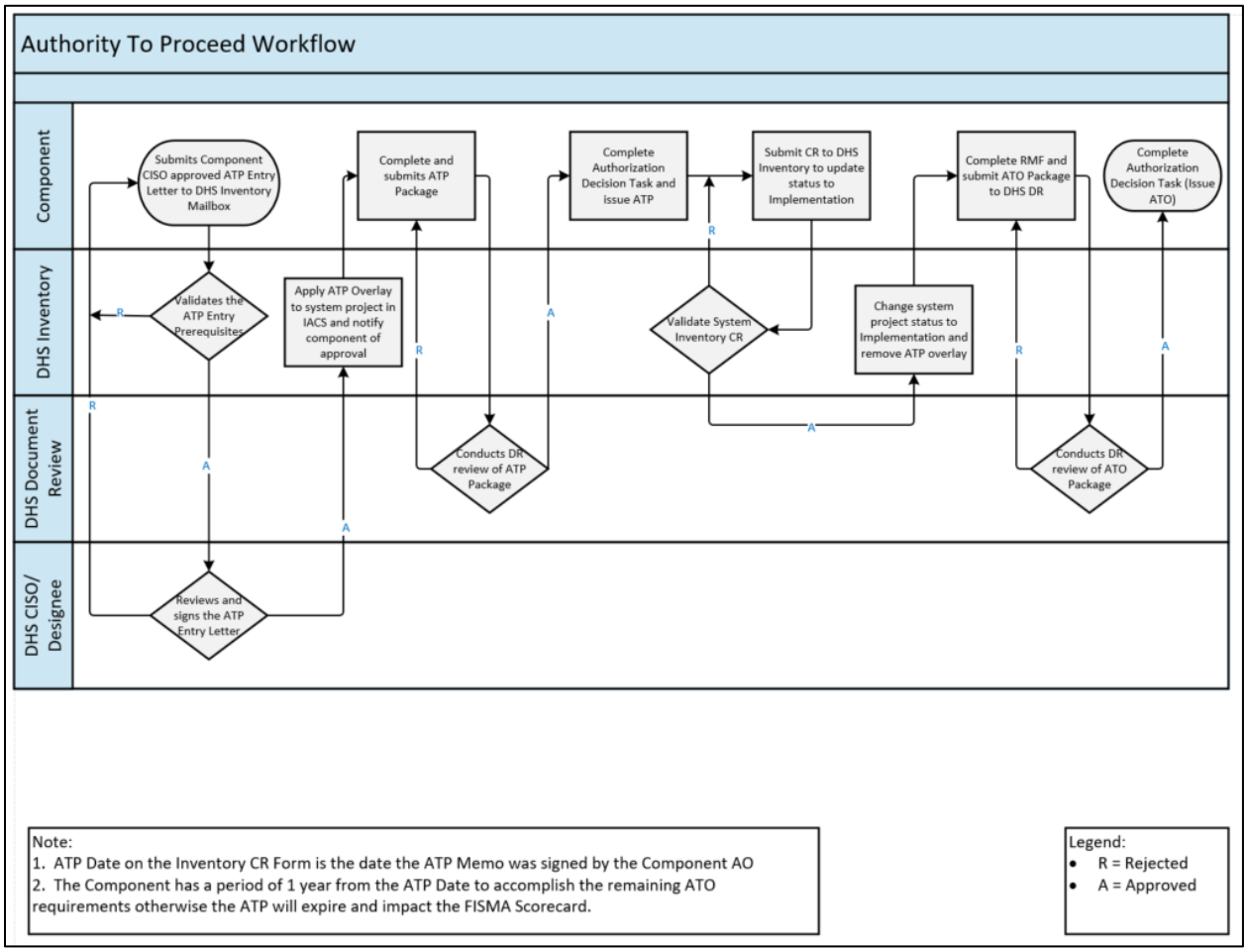

Figure 7: Swimlane diagram of ATP Workflow

The following security control set must be implemented in order to receive ATP. Additional security controls can be added at the discretion of the Components.

Table 1-ATP Baseline Controls

Controls	Title	Control Baselines
AC-2	Account Management	L / M [1,2,3,4]
AC-3	Access Enforcement	L / M
AC-6	Least Privilege	M [1,2,5,9,10]
AC-11	Session Lock	M [1]
AC-17	Remote Access	L / M [1,2,3,4]
AU-2	Audit Events	L / M [3]
AU-6	Audit Review, Analysis, and Reporting	L / M [1,3]
CA-3	System Interconnections	L / M [5]

Controls	Title	Control Baselines
CA-5	Plan of Action Milestones	L / M
CA-7	Continuous Monitoring	L / M [1]
CM-2	Baseline Configuration	L / M [1,3,7]
CM-6	Configuration Settings	L / M
CM-7	Least Functionality	L / M [1,2,4]
CM-8	Information System Inventory	L / M [1,3,5]
IA-2	Identification and Authentication (Organizational Users)	L [1,12] / M [1,2,3,8,11,12]
IR-4	Incident Handling	L / M [1]
IR-5	Incident Monitoring	L / M
IR-6	Incident Reporting	L / M [1]
PL-2	System Security Plan	L / M [3]
PL-8	Information Security Architecture	M
RA-2	Security Categorization	L / M
RA-3	Risk Assessment	L / M
RA-5	Vulnerability Scanning	L / M [1,2,5]
SA-9	External Information System	L / M [2]
SA-11	Developer Security Testing Evaluation	M
SC-7	Boundary Protection	L / M [3,4,5,7]
SC-8	Transmission Confidentiality and Integrity	M [1]
SC-12	Crypto Key Establishment and Management	L / M
SC-13	Cryptographic Protection	L / M
SC-18	Mobile Code	M
SC-28	Protection of Information at Rest	M
SI-2	Flaw Remediation	L / M [2]
SI-3	Malicious Code Protection	L / M [1,2]
SI-4	Information System Monitoring	L / M [2,4,5]
SI-10	Information Input Validation	M

APPENDIX C – EXTERNAL INFORMATION SYSTEMS

1.0 INTRODUCTION

An EIS is an information system or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness.

External information systems include:

- personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants);
- privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); information systems owned or controlled by nonfederal governmental organizations; and
- Federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations.

Before the system can be added to IACS, a request must be submitted to the DHS Inventory team with the Inventory Change Request Form. The Inventory Team will review and process the form and assign a unique FISMA ID to the EIS. In addition, the system will be added in IACS. The Component personnel do not have any function beyond providing accurate information on the system currently. Please refer to the DHS Inventory Methodology for more information.

2.0 IACS WORKFLOW ENTRY

OCISO has developed an EIS-specific RMF-workflow within the IACS Security Authorization tool. This workflow contains many process steps that are familiar to ISSOs, because they are pulled directly from the same workflow used for a GSS or MAJ. Of note, many individual process steps were removed, as they are unnecessary to complete an EIS workflow at this time, as only a few controls exist within the security control baseline. The ISSM has oversight responsibility, and approves tasks as the ISSO completes them.

Components working on an EIS should complete their FIPS designations, ISAs, and Privacy Threshold Analyses, which should be submitted to the Privacy Office. The PTAs and PIAs, if completed, can be uploaded into IACS as project artifacts, and should be used to satisfy the Privacy Tasks in IACS. PTAs are required per DHS Sensitive Systems Policy Directive 4300A policy element 3.14.1.a. ISSOs may NOT approve the Privacy task within the workflow. That task is reserved for the Privacy Office.

Components that are able to review the hosting EIS/GSS/MAJs' Security Plan should determine which controls may need to be integrated into their security baseline, which can be marked "Fully Inherited" from the hosting system, or may be marked "Partially Inheritable" or "System

Specific." If controls are inherited from the EIS/GSS/MAJ, ensure that sufficient documentation exists, and is uploaded as artifacts into IACS in order to proceed through the Security Authorization process.

DHS 4300 Attachment R pertains to not only Chief Financial Officer (CFO) designated systems, but EISs in Section 3.2. The EIS-baseline contains a set of 12 controls derived from *DHS 4300 Sensitive Systems Handbook* Attachment R Table 2. If necessary, additional controls may be integrated into the baseline using the Controls Applicability process step within IACS. However, none of the baseline controls can be removed. If any of those controls are not applicable to the EIS, the ISSO should document the reasoning, and the ISSM should ensure the accuracy of the statements prior to approving the Controls Implementation task.

For EISs, Components will need to document implementation of 12 security controls from 4300A Attachment R (Table 2 below). Components may tailor in additional controls as needed.

Table 2-EIS Applicable Controls

Control Number	Control Title
AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-3	Access Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
IA-1	Identification and Authentication Policy and Procedures
IA2	Identification and Authentication (Organization Users)
IA-4	Identifier Management
IA8	Identification and authentication (Non-Organizational Users)
PS-4	Personnel Termination
PS-5	Personnel Transfer
SA-9	External Information System Services

CP, CPT, CMP and SAP will not be applicable or required.

Component AOs will not be required to issue ATOs for EISs. However, Component ISSMs will be responsible for coordinating with their respective AOs in the event where an assessment of an EIS presents an unacceptable level of risk.

EISs will not require an Authorization Decision in IACS and will be assessed annually using the Self-Assessment Task. In addition, EISs will not be enrolled in the OA Program.

3.0 COMMON CONTROLS AND RECIPROCITY

If an Enterprise EIS becomes authorized by a Component, and will be leveraged by other DHS Components, security controls — or portions of security controls — it may be marked as "Inheritable" or "Hybrid" within the IACS-tool in the same way MAJ and GSS systems are today.

The control implementation statements should clearly mark how the EIS Owner is implementing the control, separately document how they are providing the common control for inheritance, and determine whether or not the customer responsibilities required to fully satisfy a hybrid-control implementation exist.

For information on how to provide or inherit common controls, OCISO has published the Common Controls Implementation Guide, training slides, and a reciprocity guide. In addition, control testing and results can also be exported and shared with consumers of the common controls to review and leverage, if appropriate, as part of DHS's reciprocity initiative.

4.0 PERFORMING SECURITY SELF-ASSESSMENTS

The Security Self Assessments for EISs shall be completed annually by the ISSO. The baseline set of controls will have control expirations set to expire annually, thus requiring the assigned ISSO to re-test these controls, and update any artifacts, as needed. In addition, the ISSM shall validate that testing was completed, concur with the results of testing, and ensure that the creation, maintenance, and closure of POA&Ms are completed. Furthermore, the ISSM shall ensure that all tasks and process steps within IACS are complete prior to advancing the workflow to the Component Document Review task. Please note that the EIS-workflow in IACS does not have separate tasks for the Self-Assessment and Security Assessment. Due to the limited control, baseline, and small number of EISs in the inventory, only a single self-assessment by the ISSO, and validation by an ISSM, is necessary.

5.0 DOCUMENT REVIEW

Once the self-assessment is complete, the Component Document Review task shall be completed and approved. Next, the DHS Document Review Team will review all artifacts presented within the system, as well as the completeness of the EIS-Self Assessment published documents, based on requirements listed in the "EIS tab" within the Document Review checklists. The Document Review Team will ensure that the baseline of 12 controls have been implemented, tested, and

reviewed. Systems providing Common Controls will be subject to further review to ensure that shared responsibilities of controls are properly documented from both a provider and a consumer perspective.

6.0 WORKFLOW COMPLETION

After Component and DHS Document Review tasks are complete, and the ISSO has completed all tasks within the Security Authorization tool, the workflow completion task shall be marked "Complete" with the current date.

APPENDIX D – REFERENCES

Federal Laws

Federal Information Security Management Act of 2002 (FISMA), 44 USC 3541 et seq., enacted as Title III of the E-Government Act of 2002, Pub L 107-347, 116 Stat 2899 [see also FISMA 2014]

Federal Information Security Modernization Act of 2014 (FISMA 2014), Public Law 113-283, 128 Stat 3087

Office of Management and Budget (OMB) Circulars

OMB Circular A-123, "Management's Responsibility for Internal Control", Revised, December 21, 2004 [Note: Portions of this document have been paused, and portions modified, by M-17-26, "Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda," June 15, 2017]

OMB Circular A-130 Revised, "Management of Federal Information Resources," July 28, 2016

DHS Information Security Policy Documents

[The most current versions are found on the CISO Security Documents page]

DHS Sensitive Systems Policy Directive 4300A, v13.1, July 27, 2017

DHS 4300A Sensitive Systems Handbook, v12, November 15, 2015

Attachments to DHS 4300A *Sensitive Systems Handbook*, particularly:

Attachment B, "Waiver Requests"

Attachment C, "Information Systems Security Officer (ISSO) Designation Letter"

Attachment D, "Type Accreditation"

Attachment E, "FISMA Reporting"

Attachment F, "Incident Response"

Attachment G, "Rules of Behavior"

Attachment H, "Plan of Action and Milestones (POA&M) Process Guide"

Attachment K, "IT Contingency Plan Template"

Attachment M, "Tailoring NIST 800-53 Security Controls"

Attachment N, "Preparation of Interconnection Security Agreements"

Attachment O, "Vulnerability Management"

Attachment P, "Document Change Requests"

Attachment Q1, "Wireless Systems"

Attachment Q2, "Mobile Devices"

Attachment Q3, "Tactical Systems"

Attachment Q4, "RFID Systems"

Attachment Q5, "Voice over Internet Protocol (VoIP)"

Attachment Q6, "Bluetooth Security"

Attachment Q7, "International Travel with Mobile Devices"

Attachment R, "Compliance Framework for CFO-designated Systems"

Attachment S, "Compliance Framework for Privacy Systems"

Attachment S1, "Managing CREs Containing SPII"

Attachment T, "Acronyms"

Attachment X, "Social Media"

Other DHS Guidance

DHS Ongoing Authorization Methodology

DHS Common Control Implementation Guide v2.2

DHS CISO Security Controls tri-fold

DHS FISMA System Inventory Methodology

DHS Information Security Performance Plan

DHS Document Review Methodology

Document Review Checklists

Security Authorization Document Templates

Privacy Threshold Analysis (PTA) Template

Additional references that may be useful when conducting a Security Authorization include:

Component specific guidance

DHS Information System Security Officer (ISSO) Guide

Telos Xacta User Guide and In-application Help

NIST Publications; latest revisions may be found at https://csrc.nist.gov/publications

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*

Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*

FIPS-199 Workbook and Instructions

Framework for Improving Critical Infrastructure Cybersecurity v1

NIST Special Publications (SPs) in the 800 series, especially:

SP 800-18, Rev 1, "Guide for Developing Security Plans for Federal Information Systems," February 24, 2006

SP 800-30, Rev 1, "Guide for Conducting Risk Assessments," September 17, 2012

SP 800-34, Rev 1, "Contingency Planning Guide for Information Systems," November 11, 2010

SP 800-37, Rev 2, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," June 10, 2014) [Note that Rev 1 is still available from NIST but will be withdrawn December 20, 2019] SP 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 1, 2011

SP 800-53A, Rev 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," December 18, 2014

SP 800-60, Vol. 1 Rev 1, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 1, 2008

SP 800-60, Vol. 2 Rev 1, "Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices," August 1, 2008SP 800-160, Vol. 1, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," March 21, 2018 [Vol. 2, covering Cyber Resiliency Considerations also March 21, 2018, in DRAFT

APPENDIX E – FEDRAMP REFERENCES

References specific to FedRAMP can be found at https://www.fedramp.gov/documents/, including the following:

FedRAMP ATOs

- FEDRAMP Policy Memo
- Agency Authorization - Best Practices for CSPs
- Agency Authorization – Roles and Responsibilities for FedRAMP, CSPs, and Agencies
- FedRAMP General Document Acceptance Criteria
- Significant Change Policies and Procedures
- Security Assessment Framework
- Timelines and Accuracy of Testing Requirements
- Control Specific Clauses

FedRAMP Requirements for Agency and JAB Authorized Systems

- Assessors
- Annual Assessment Guidance
- Security Assessment Framework
- Annual Assessments Controls Selection Worksheet
- Incident Communications Procedures
- FedRAMP Security Controls Baseline
- FedRAMP Guide for Multi-Agency Continuous Monitoring
- Vulnerability Scan Requirements
- Continuous Monitoring Performance Management Guide
- Agency Authorization: Obtaining In Process Designation
- Agency Authorization Playbook

Additional FedRAMP References

- FedRAMP Master Acronym and Glossary
- Additional Guidance

APPENDIX F – ACRONYMS AND ABBREVIATIONS

Acronym	Definition
3PAO	Third Party Assessment Organization
AISSO	Alternate Information System Security Officer
AO	Authorizing Official
ATO	Authority to Operate
ATP	Authority to Proceed
BIA	Business Impact Analysis
BRM	Business Reference Model
CAT	Control Allocation Table
CCB	Change Control Board
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMP	Configuration Management Plan
CP	Contingency Plan
CPIC	Capital Planning and Investment Control
CPO	Chief Privacy Officer
CPT	Contingency Plan Test
CRE	Computer-Readable Extract
CRMC	Cybersecurity Risk Management and Compliance
CSO	Chief Security Officer
CSP	Cloud Service Provider
DBA	Database Administrator
DHS	Department of Homeland Security
DOD	Department of Defense
DR	Document Review
eAuth	E-Authentication
EBMO	Enterprise Business Management Office
EEPROM	Electrically Erasable Programmable Read-Only Memory
EIS	External Information System
FDCC	Federal Desktop Core Configuration
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FISMA 2014	Federal Information Security Modernization Act
FOIA	Freedom of Information Act

Acronym	Definition
FOUO	For Official Use Only
FSO	Facility Security Officer
GSA	General Services Administration
GSS	General Support System
HQ	Headquarter
HVA	High Value Asset
IaaS	Infrastructure as a Service
IACS	Information Assurance Compliance System
IATO	Interim Authorization to Operate
IDS	Intrusion Detection System
IM	Inventory Management
IoT	Internet of Things
IPS	Intrusion Prevention System
ISA	Information Security Agreement
ISCM	Information Security Continuous Monitoring
ISO	Information Security Office
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISVM	Information Security Vulnerability Management
IT	Information Technology
JAB	Joint Authorization Board
LAN	Local Area Network
MA	Major Application
MES	Mission Essential System
MFA	Multifactor Authentication
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NSS	National Security Systems
NSSD	National Security Systems Division
OA	Ongoing Authorization
OCISO	Office of the Chief Information Security Officer
OMB	Office of Management and Budget
ORMB	Operational Risk Management Board
PaaS	Platform as a Service
PATO	JAB Provisional Authorizations
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information

Acronym	Definition
PMO	Project Management Office
POA&M	Plan of Action and Milestones
PPOC	Component Privacy Officers/Privacy Points of Contact
PTA	Privacy Threshold Analysis
RA	Risk Assessment
RMF	Risk Management Framework
RTM	Requirements Traceability Matrix
SA	Security Authorization
SaaS	Software as a Service
SAF	Security Assessment Framework
SAP	Security Assessment Plan
SAR	Security Assessment Report
SBU	Sensitive but Unclassified
SCA	Security Control Assessor
SELC	System Engineering and Life Cycle
SLA	Service Level Agreement
SOC	Security Operations Center
SOP	Standard Operating Procedures
SORN	System of Records Notice
SP	Special Publication; Security Plan
SPII	Sensitive Personally Identifiable Information
TCP	Transmission Control Protocol
TRAL	Trigger Accountability Log
TT&E	Test, Training and Exercise
UII	Unique Investment Identifier
US	United States
USGCB	US Government Configuration Baseline
VoIP	Voice over Internet Protocol