Department of Commerce

Security and Privacy Assessment & Authorization (SPA&A) Handbook

Office of Cybersecurity and IT Risk Management (OCRM)

Version 1.1

Table of Contents

Revision History and Approval

Please note that when in hard copy, this document is not a controlled copy and does not necessarily reflect the latest version. This is a living document and will be subject to change due to required revisions.

Revision Log			
Version	**Date**	**Approvers**	**Changes**
1.0	03/16/2023	Director, OSPMS	Original
1.1	01/2025	Director, OSAS Director, OSPMS	Annual Review and Update

Approval Log			
Version	**Date**	**Approvers**	**Changes**
1.0	03/30/2023	CISO/DCIO, DOC	Original
1.1	01/2025	CISO/DCIO, DOC	Annual Review and update

Approval

As the Department of Commerce's (DOC) Chief Information Security Officer (CISO) / Deputy Chief Information Officer (DCIO), responsible for the management and oversight of the Enterprise Cybersecurity Program, I hereby approve the Security and Privacy Assessment & Authorization Handbook, version 1.1, for publication.

Approver Name: Ryan A Higgins

Approver Title: Department of Commerce CISO / DCIO

Approver Signature & Date: RYAN HIGGINS Digitally signed by RYAN HIGGINS Date: 2025.01.22 12:03:00 -05'00'

1 Introduction

1.1 Purpose

The Department of Commerce (Department or DOC) Chief Information Security Officer (CISO) is responsible for developing cybersecurity guidance, implementation, and oversight for DOC's Cybersecurity Program as required by the Federal Information Security Modernization Act of 2014 (FISMA). The Office of the Chief Information Officer (OCIO), Office of Cybersecurity and IT Risk Management (OCRM) has established a cybersecurity governance framework that serves as the foundation for the Department's Cybersecurity Program. The framework publishes:

- **Policy** as the primary mechanism to enforce cybersecurity requirements and define roles and responsibilities
- **Security and Privacy Control Matrix (SPCM)** to supplement policy by identifying organizationally defined control parameters, in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53
- **Standards** based on the SPCM with specific technical requirements for Cybersecurity Program areas
- **Handbooks** to guide the implementation of processes in support of the policy and SPCM

The DOC Chief Privacy Officer (CPO) is the Department's Senior Agency Official for Privacy (SAOP) and is responsible for ensuring compliance with applicable privacy requirements, developing, and evaluating privacy policy, and managing privacy risks associated with any agency activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems. Consistent with Executive Order 13719 (E.O. 13719) and OMB M-16-24, the DOC CPO is responsible for developing, implementing, maintaining, and overseeing the Department's privacy program. The DOC CPO serves as the Director of the Office of Privacy and Open Government (OPOG).

The Security and Privacy Assessment & Authorization (SPA&A) Handbook is designed for use by all DOC stakeholders for the planning and execution of the security and privacy assessment and authorization process. The SPA&A Handbook serves as the single authoritative source for the SPA&A process.

1.2 Background

OCRM oversees the Department's Cybersecurity Program and is responsible for management and oversight of the SPA&A process. The ECP assigns authority to the DOC CISO to develop and maintain cybersecurity policies, procedures, and control techniques to address all requirements for protecting the confidentiality, integrity, and availability of DOC's IT resources.

The CPO and Director of OPOG is responsible for developing and maintaining privacy policies, procedures, and guidance essential to the effective and efficient implementation of the

Department's program. This includes working with the Department's Chief Information Officer to ensure that the process for assessing and authorizing information systems appropriately addresses privacy-related issues.

Together, the DOC CISO and DOC CPO ensure that the Department develops cybersecurity and privacy policies consistent with applicable statutory authority, such as the Clinger-Cohen Act, FISMA, Privacy Act of 1974, and E-Government Act, and in accordance with Office of Management and Budget (OMB) mandates, Committee on National Security System Policy (CNSSP), Intelligence Community Directives (ICD), Federal Information Processing Standards (FIPS), NIST publications, and DOC policy.

The SPA&A Handbook will guide system stakeholders in securing, managing, and reporting on information and information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of DOC information. In addition, the Handbook documents the process for executing the NIST Risk Management Framework (RMF), NIST Cybersecurity Framework (CSF), CNSSP, and ICD.

> "*The unified and collaborative approach to bring security and privacy evidence together in a single authorization package will support authorizing officials with critical information from security and privacy professionals to help inform the authorization decision. In the end, it is not about generating additional paperwork, artifacts, or documentation. Rather, it is about ensuring greater visibility into the implementation of security and privacy controls which will promote more informed, risk-based authorization decisions.*"
>
> - *NIST SP 800-37 (Rev.2)*

1.3 Scope and Applicability

The scope of the SPA&A Handbook is to outline the RMF and to provide direction for performing SPA&A activities on all information systems supporting the DOC (Office of the Secretary and operating units[1]). The SPA&A Handbook is applicable to all DOC unclassified and classified information and information systems including cloud information systems, contractor-operated DOC information systems (i.e., systems that are DOC-owned but operated by contractors), and externally operated systems (i.e., systems that are outside of DOC control) that collect, process, transmit, store, and disseminate DOC information. Operating unit policy supplementation,

[1] The operating units of the Department are organizational entities outside the Office of the Secretary charged with carrying out specified substantive functions (i.e., programs) of the Department. *See* Department Organizational Order (DOO) 1-1, *Mission and Organization of the Department of Commerce*.

including any policies or procedures that are more stringent, must depend on mission and risk-based requirements.

In accordance with FISMA and OMB Circular No. A-130, all unclassified information and information systems are expected to be developed, operated, and maintained in compliance with NIST standards and guidelines, and all classified information systems are expected to be in compliance with Committee on National Security Systems (CNSS) security standards immediately upon deployment of the system.

The SPA&A Handbook is designed to secure information systems within DOC and support enterprise risk management by ensuring that security and privacy is included and considered from system initiation until disposal. The SPA&A Handbook enables consistent, comparable, and repeatable assessments of security and privacy controls in DOC information systems and promotes a better understanding of DOC and operating unit-related mission risks resulting from the operation of information systems.

1.4 Authorities: Statutes, Federal Mandates, Department Mandates and Federal Guidance

This Handbook has been developed in accordance with the following authorities and references:

1.4.1 Statutes

- United States Congress: E-Government Act of 2002, Section 208 (Public Law 107-347)
- United States Congress: Federal Information Security Modernization Act of 2014 (Public Law 113-283)
- United States Congress: Paperwork Reduction Act of 1995 (Public Law 104-13)
- United States Congress: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Public Law 107-56)
- United States Congress; Cybersecurity Act of 2015 (Public Law 114-113, Division N)
- United States Congress; Federal Information Technology Acquisition Reform Act of 2014 (Public Law 113-291)
- United States Congress; Information Technology Management Reform Act of 1996 (Public Law 104-106)
- United States Congress: Privacy Act of 1974 (Public Law 93-579), as amended

1.4.2 Department Mandates

- Department Administrative Order (DAO) 200-0: *Department of Commerce Handbooks and Manuals*
- DAO 207-1: *Security Programs*
- Department Organizational Order (DOO) 15-23: *Chief Information Officer*

- DOO 1-1: *Mission and Organization of the Department of Commerce*
- DOO 20-31: *Chief Privacy Officer and Director of Open Government*
- DOC Enterprise Cybersecurity Policy (ECP)
- DOC Information Security Continuous Monitoring (ISCM) Handbook
- DOC Configuration Management (CM) Standard
- DOC Incident Response Management Standard (IRMS)
- DOC Vulnerability Management (VM) Standard
- DOC Plan of Action and Milestones (POA&M) Handbook
- DOC High Value Asset (HVA) Handbook

1.4.3 Federal Guidance

- Executive Order 13719: *Establishment of the Federal Privacy Council, February 2016*
- NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems, February 2004*
- NIST SP 800-60 Vol. 1 Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008*
- NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide, August 2012*
- NIST SP 800-145, *The NIST Definition of Cloud Computing September 2011*
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010*
- NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Information Technology Systems, February 2006*
- NIST SP 800-161 Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, May 2022*
- NIST SP 800-30 Rev. 1, *Risk Management Guide for Information Technology Systems, September 2012*
- NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems, May 2010*
- NIST SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018*
- NIST SP 800-39 *Managing Information Security Risk March 2011*
- NIST SP 800-47 Rev. 1, *Managing the Security of Information Exchanges*, *July 2021*
- NIST SP 800-50 *Building an Information Technology Security Awareness and Training Program, October 2003*

- NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations, September 2020*

1.4.4 Federal Mandates

- Office of Management and Budget (OMB) Circular A-108: *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act, December 2016*
- OMB Circular A-130: *Managing Information as a Strategic Resource, July 2016*
- OMB Memorandum-02-01: *Guidance for Preparing and Submitting Security Plans of Action and Milestones, October 17, 2001*
- OMB M-04-04: *E-Authentication Guidance for Federal Agencies, December 2003*
- OMB M-16-24: *Role and Designation of Senior Agency Officials for Privacy, September 2016*
- OMB M-17-09: *Management of Federal High Value Assets, December 9, 2016*
- OMB M-24-15: *Modernizing the Federal Risk and Authorization Management Program, July 2024*
- OMB M-23-16: Update to Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practice, June 2023*
- Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience, February 12, 2013*

1.5 Waivers

Operating units requesting to waive requirements established in the DOC ECP, the SPCM, a DOC Standard, or a DOC Handbook, due to adverse impact on mission, business, or operations must follow the Cybersecurity Policy Waiver Process[2].

Waivers provide a mechanism for DOC OCIO to track, monitor, and ensure the proper management of residual risks introduced by a waived requirement. Types of acceptable risk for consideration are based upon DOC and operating unit priorities and trade-offs between: (i) near-term mission/business needs and potential for longer-term mission/business impacts; and (ii) the Department's interests and the potential impacts on individuals, other organizations, and the Nation.[3] The DOC OCIO will coordinate the review of waiver requests with the DOC CPO to ensure that any requested waivers take into consideration privacy compliance and potential privacy risks.

[2] Cybersecurity Policy Waiver Process | Commerce Connection

[3] NIST SP 800-39, *Managing Information Security Risk*

1.6 Effective Date

This Handbook is effective upon final approval and issuance. OCRM, in coordination with OPOG, will review the SPA&A Handbook annually and make updates as necessary.

2 Roles and Responsibilities

Roles and Responsibilities for the SPA&A Handbook are in the supplemental SPA&A Appendix C: Roles and Responsibilities.

3 SPA&A Lifecycle

The integration of the SPA&A process and DOC System Development Lifecycle (SDLC) increases the probability that security and privacy features manage privacy risks and meet the necessary confidentiality, integrity, and availability objectives, resulting in a successful authorization. The Cyber Security Assessment and Management (CSAM) application supports every step in the RMF and provides procedures and supplemental guidance to develop the required SPA&A documentation. In alignment with OMB Circular No. A-130 (as revised in 2016), the execution of the following seven steps is essential to obtain an Authorization to Operate (ATO):

- **Prepare** to execute the RMF from an organization-level and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
- **Categorize** the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss of integrity, availability, and confidentiality.
- **Select** an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.
- **Implement** the controls and describe how the controls are employed within the system and its environment of operation.
- **Assess** whether the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
- **Authorize** the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
- **Monitor** the system and the selected controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

Figure 3.1: SPA&A Lifecycle Example

4 SPA&A Content

The following sections will explain in detail the process for completing the RMF activities, along with necessary artifacts and outcomes.

4.1 RMF Step 0 - Prepare (Organizational Level)

The Prepare tasks P-1 through P-7 establish the context and priorities for managing Department and operating unit level security and privacy risks. In accordance with NIST SP 800-37 Rev. 2, it is recommended that operating units assign internal risk management roles, activities, system stakeholders, and security and privacy roles as outlined in the SPA&A Handbook before beginning the information system assessment and authorization process. The review of privacy risks begins during this step and the development stages of actions and policies that involve information systems managing Personally Identifiable Information (PII) or Business Identifiable Information (BII) continue throughout the information system's lifecycle.

Table 4-1: Prepare Step Task Details

Task	Activity	Outcome
Task P-1: Risk Management Roles	Identify and assign individuals to specific roles associated with security and privacy risk management	Defined formal RMF roles and responsibilities
Task P-2: Risk Management Strategy	Establish a risk management strategy for the organization that includes a determination of risk tolerance	Enterprise-wide risk management strategy and statement of risk tolerance
Task P-3: Risk Assessment	Assess organization-wide security and privacy risk and update the assessment results on an ongoing basis	Enterprise and operating unit level risk assessment results accessible in CSAM
Task P-4: Tailored Control Baselines	Establish, document, and publish organizationally tailored control baselines and/or Cybersecurity Framework Profiles	DOC SPCM with tailored control baselines; CSF Profile in CSAM
Task P-5: Common Control Identification	Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems	DOC and operating unit level Security and Privacy Common Control Programs and System Security and Privacy Plan (SSPP) available for inheritance
Task P-6: Impact-Level Prioritization	Prioritize organizational systems with the same impact level	Defined security impact levels along with system profile designation such as HVA, Critical Infrastructure, Financial, High, Moderate, and Low

Task	Activity	Outcome
Task P-7: Continuous Monitoring Strategy	Develop and implement an organization-wide strategy for continuously monitoring control effectiveness	An implemented organizational Information Security Continuous Monitoring (ISCM) and PCM Strategy

4.1.1 RMF Task P-1 Risk Management Roles

OCRM serves as the focal point for cybersecurity in DOC. OCRM provides DOC-wide management and implementation of the Department's Cybersecurity Program in accordance with FISMA and Federal Risk and Authorization Management Program (FedRAMP). In accordance with DOO 20-31, and consistent with E.O. 13719, OMB M-16-24, and OMB Circular A-130, the DOC CPO and OPOG provide DOC-wide oversight of the Department's privacy program. This includes the establishment and operation of privacy programs and privacy officials within the Department's operating units.

Operating units must ensure that role assignments to individuals, groups, or offices have sufficient understanding and expertise to fulfill the responsibilities associated with the role and that there are no conflicts of interest when assigning the same individual to multiple risk management roles. For example, authorizing officials (AOs) cannot occupy the role of system owner (SO) or common control provider for systems or common controls they are authorizing. In addition, combining multiple roles for security and privacy requires care because the two disciplines may require different expertise, and in some circumstances, the priorities may be competing.

4.1.2 RMF Task P-2 Risk Management Strategy

The DOC Enterprise Risk Management (ERM) Program includes the establishment of organizational risk tolerance, acceptable risk assessment methodologies, risk response recommendations, a process for consistently evaluating security and privacy risks enterprise-wide and approaches for monitoring risk over time. Risk framing must be done at the Department and operating unit levels to appropriately drive IT investment, enterprise architecture, and the implementation of security and privacy controls.

The cybersecurity representatives of the DOC ERM Council will evaluate cybersecurity risks and input as necessary into the Department's risk register and profile. Operating units must adhere to the enterprise-wide risk management approach and can create supplemental procedures, when necessary, to analyze, prioritize risks, and provide a foundation for response and monitoring at the operating unit or information system level. Refer to the C-ERM for more information on the enterprise risk management strategy.

Cybersecurity risk framing establishes the environment in which risk decisions are made, and includes four key tasks:

- Define risk assumptions concerning threats, vulnerabilities, consequences and impacts, and likelihood of occurrence
- Identify constraints at all three DOC ISCM Tiers:
  - Level 1: Department
  - Level 2: Operating unit
  - Level 3: Information System
- Determine risk tolerance and risk appetite in a way that can be interpreted at all levels; risk tolerance and risk appetite are guideposts that set strategy
- Identify requirements, priorities, and trade-offs, protecting HVAs, primary mission functions, and PII/BII

4.1.3 RMF Task P-3 Risk Assessment

The DOC enterprise-level risk assessment results are aggregated information from the operating unit and system-level risk assessment results, continuous monitoring, and any strategic risk considerations relevant to the Department. DOC considers the totality of risk from the operation and use of its information systems from exchanges and connections with other internally and externally owned systems, and external providers' use. DOC and operating units may also consider the variability of different offices and programs such as personnel security, physical security, and acquisitions within the organization and the need to account for such disparities.

The Department requires the use of CSAM and the Enterprise Continuous Diagnostics and Monitoring (ECDM) capabilities to provide a holistic real-time enterprise view of DOC's cybersecurity posture within all three ISCM Tiers. DOC captures and tracks cybersecurity and privacy risk assessments for information systems in CSAM.

In accordance with DOC's cybersecurity strategy, every ISCM Tier must ensure risk assessments are complete and support DOC's continuous monitoring program. The DOC requires that all assets must be tagged with their respective CSAM ID sequence number for maintaining an identifiable asset inventory. CSAM IDs are the unique identifiers for FISMA authorization boundaries.

In alignment with the requirements from DHS for the ECDM program, each asset/endpoint needs to be assigned to a FISMA container to identify the system boundaries and track assets assigned to those boundaries. With the Department's asset tagging capability, information can be monitored at a granular level, which provides a method for tracking the asset owner, system designation (i.e., Mission Essential System (MES)), Critical Infrastructure, Financial System, and HVA) to mission/business processes and enterprise-level risks. This comprehensive inventory assists DOC and operating units with determining which assets need assessment priority and risk mitigation.

DOC operating units can use risk assessments to support decision-making regarding:

- Development of an information security architecture
- Adherence to and periodic reviews of Memorandum of Understanding/Agreement (MOU/A) and Interconnection Security Agreement (ISA) requirements

- Design, implementation, operation and maintenance of security technologies and solutions
- Selection of Supply Chain Risk Management (SCRM) controls
- Authorization or denial of ATO information systems
- Modification of missions/business functions and/or processes
- Funding of information security programs

DOC uses CSAM, automated, and manual cybersecurity capabilities to monitor and report on the enterprise security posture. These tools and capabilities can assist with evaluating compliance with the implementation of the RMF. The RMF operates primarily at DOC's ISCM and PCM Tier 3 with some applications at Tier 1 and 2. This shared risk management responsibility provides a holistic risk management view and the identification and implementation of DOC's Common Controls Program.

DOC assesses risks on an ongoing basis with frequencies defined in the DOC ISCM Handbook[4]. Additional and ad-hoc risk assessments may be required in response to a major cybersecurity incident, at the direction of the DOC CIO and CISO based upon Binding Operational Directives (BOD) and Emergency Directives (ED) issued by the Department of Homeland Security (DHS), or when threats and triggers are discovered during the risk monitoring process. Similarly, additional and ad-hoc risk assessments may be required when a major incident constitutes a breach, at the direction of the DOC CPO based upon OMB guidance. Operating units must conduct risk assessments during all phases of the SDLC to detect security and privacy control deficiencies early and to initiate corrective action in a more cost-effective manner.

4.1.4 RMF Task P-4 Tailored Control Baselines/Cybersecurity Framework Profiles

The DOC security control baselines and tailoring guidance aligns with the NIST SP 800-60 guidance for unclassified systems. DOC implements security control overlays, as appropriate, which complement the NIST and CNSS minimum security control baselines and provides an opportunity to add or tailor-out controls to accommodate unique mission, business, and operational requirements.

The DOC Security and Privacy Controls Matrix (SPCM) documents the minimum baseline security controls for High, Moderate, and Low security impact systems with defined control parameters for selected controls and control enhancements through the DOC Common Control Program (CCP). While not required, operating units can establish more stringent security control requirements to supplement the DOC cybersecurity standards and handbooks. However, operating units may not establish less stringent requirements.

[4] Find ISCM Handbook at Enterprise Cybersecurity Policy Program | Commerce Connection.

4.1.5 RMF Task P-5 Common Control Identification

An enterprise-wide view of security and privacy controls allows the SO to identify resources needed to protect their information assets while also managing privacy risks. Security and privacy controls are designated as:

- Program management controls (i.e., controls that are generally implemented at the agency level and are independent of any particular information system)
- Common controls (i.e., controls that provide a security and privacy capability for multiple information systems)
- Hybrid controls (i.e., controls that have both system-specific and common characteristics)
- System-specific controls (i.e., controls that provide a security and privacy capability for a particular information system only).

Allocating security and privacy controls into one of these three categories will establish a baseline of common, hybrid, and system-specific controls. The SO offering the security control for inheritance becomes the "common control provider" for that control. A SO cannot offer a control for inheritance if inheriting the control from another source and/or the SO is not the common control provider. The DOC CPO is responsible for designating which privacy controls the Department will treat as program management, common, information system-specific, and hybrid controls. A common control can apply to all DOC information systems, a group of information systems at a specific site, a subsystem, or an application deployed at multiple operational sites with similar business and mission needs. Implementing common control(s) will foster a more efficient and consistent IT management approach, increased coordination among key stakeholders, and more disciplined governance for the Department. The use of common controls will reduce the cost of conducting security and privacy authorizations by taking advantage of shared services.

As defined by NIST, "a common control provider is an organizational official responsible for the development, implementation, assessment, and monitoring of common controls[5]". The common control provider can be an individual system, group, or organization responsible for the development, implementation, assessment, and monitoring of the security or privacy controls offered for inheritance. Common control providers must:

- Document the common controls in a SSPP
- Ensure that required assessments of the security and privacy controls are conducted
- Document assessment findings in a Security and Privacy Assessment Report (SPAR)
- Produce a Plan of Action and Milestones (POA&M)[6] for all controls having deficiencies
- Receive authorization from the AO or DOC CPO to offer common controls
- Monitor common control effectiveness on an ongoing basis

[5] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[6] See DOC POA&M Handbook at Enterprise Cybersecurity Policy Program | Commerce Connection.

SOs may request CSAM access to SSPPs, SPARs, and POA&Ms for common controls (or a summary of such information) after obtaining formal approval from the CCP AO, DOC CPO, or designated authority.

Similar to a common control, a hybrid security control is where a portion of the control implementation is the responsibility of the SO, while the remaining control implementation is common and provided by the common control provider. The intent of hybrid controls is to allow a SO to implement and assess parts of the security or privacy control under their direct management and inherit other portions that are managed by the common control provider. A system-specific control is under the direct management of the information system. During the control selection process, SOs must implement system-specific applicable controls and meet the unique system requirements.

When utilizing external shared services, operating units must establish agreements with service providers and evaluate information on the service provider-offered controls' effectiveness.

4.1.6 RMF Task P-6 Impact-Level Prioritization

Unclassified systems apply the high-water mark concept to determine an appropriate categorization level. Classified systems apply the CNSS 1253 baselines for the national security information systems. Operating units requiring further categorizations can prioritize their systems within impact levels. Operating units use impact-level prioritization to determine which systems are critical or essential to missions and operations to allocate resources appropriately based on complexity, aggregation, and system interconnections. Operating units can conduct impact-level prioritizations at any level. Individual SOs report security categorization data for the basis of impact-level prioritizations.

4.1.7 RMF Task P-7 Continuous Monitoring Strategy

An important aspect of risk management is the ability to monitor the security posture across the enterprise and the effectiveness of controls on an ongoing basis. Continuous monitoring strategies also include supply chain risk considerations. The DOC ISCM Program addresses monitoring requirements at all Tiers. DOC defines and publishes the annual Core Control assessment requirement at the enterprise level via the DOC SPCM. Operating units must ensure appropriate assessment, monitoring, and risk management of select controls, in addition to the Department Core Controls. In support of DOC's ECP, the DOC ISCM Strategy defines the minimum monitoring frequency for security controls and ongoing control assessment requirements.

4.2 RMF Step 0 – Prepare (System Level)

The Prepare tasks P-8 through P-18 establish the context and priorities for managing information system security and privacy risks. During this phase, the SO is required to complete the preparation activities prior to starting the later phases of the RMF.

Table 4-2: Prepare Task Activity List

Task	Activity	Outcome
Task P-8: Mission or Business Focus	Identify the missions, functions, and processes that the system is intended to support	Missions, functions, and processes that the system supports are defined
Task P-9: System Stakeholders	Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system	System stakeholders are documented in the SSPP
Task P-10: Asset Identification	Identify assets that require protection	Inventory of hardware, software, and firmware are managed, and assets are tagged
Task P-11: Authorization Boundary	Determine the authorization boundary of the system	Clearly document and define the system authorization boundary in a network architecture diagram and upload into CSAM
Task P-12: Information Types	Identify the types of information to be processed, stored, and transmitted by the system	Select from NIST SP 800-60 and FIPS 199 the information types for the system in CSAM
Task P-13: Information Life Cycle	Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system	Documentation of the stages through which information passes in the system are uploaded into CSAM. If the system processes PII, a data flow diagram (i.e., data map) illustrating how PII is processed throughout the information lifecycle is required
Task P-14: Risk Assessment - System	Conduct a system-level risk assessment and update the results on an ongoing basis	Security and privacy risk assessment reports are available in CSAM.
Task P-15: Requirements Definition	Define the security and privacy requirements for the system and the environment of operation	Documented security and privacy requirements using NIST SP 800-53 Rev. 5 and NIST SP 800-161 (as applicable) control set
Task P-16: Enterprise Architecture	Determine the placement of the system within the enterprise architecture	Updated enterprise and security architecture, privacy policy, plans to use cloud-based and shared systems, services, or applications

Task	Activity	Outcome
Task P17: Requirements Allocation	Allocate security and privacy requirements to the system and to the environment of operation	List of minimum-security baseline requirements allocated to the system List of privacy requirements allocated to the system
Task P-18: System Registration	Register the system with the program or management offices	Information System Registration Form

4.2.1 RMF Task P-8 Mission or Business Focus

DOC missions and business functions influence the design, development, and implementation of information systems and programs. They also drive cybersecurity initiatives, investment strategies, funding decisions, resources, and risk decisions. The Department follows guidance contained in the OMB publications: The Common Approach to Enterprise Architecture, and the Federal Enterprise Architecture Framework (FEAF). These two documents provide direction for the development and content of Enterprise Architectures (EA) to maintain consistency across the Federal Government. DOC stakeholders participate in the development of the EA to acquire a thorough understanding of the various operating unit missions, business functions, and processes from system security and privacy perspectives.

4.2.2 RMF Task P-9 System Stakeholders

Operating units must identify stakeholders that have an interest throughout the system life cycle - for design, development, implementation, delivery, operation, and sustainment of the system, including all aspects of the supply chain. Stakeholders must communicate with each other during every step in the RMF to ensure that they satisfy security and privacy requirements, address concerns and issues expeditiously, and carry out risk management processes effectively.

4.2.3 RMF Task P-10 Asset Identification

Operating units must identify assets requiring protection based on stakeholder concerns and the context of their use, complying at a minimum, with the FIPS 199 Confidentiality, Integrity, and Availability ratings. Effectively monitoring and managing information system assets support the clear identification of an authorization boundary and necessary safeguards to secure the asset. All assets must be tagged with their respective CSAM ID sequence number using the BigFix tagging solution.

Information assets can be tangible or intangible assets and can include the information needed to carry out missions or business functions, deliver services, and system management/operations. In addition to hardware, software, and firmware assets, tangible information assets can include Controlled Unclassified Information (CUI) and all forms of information system documentation.

4.2.4 RMF Task P-11 Authorization Boundary

Authorization boundaries establish the scope of protection for information systems. AOs determine authorization boundaries with input from the SO. A clear delineation of authorization boundaries is important for accountability and security categorization. Each system includes a set of elements that support the organization's missions and business processes. System elements include human, technology/machine, and physical/environmental elements. The term system defines the set of system elements, interconnections, and the environment that is the focus of the RMF/CSF implementation.

For information systems processing PII or BII, it is important for the privacy and security programs to collaborate and develop a common understanding of authorization boundaries. Privacy and security programs provide a consistent understanding of the authorization boundary to conduct risk assessments and select controls. In some cases, formal agreements (contractual, MOU/ISA, etc.) with external providers are required to delineate ownership and ensure accountability for the information system.

4.2.5 RMF Task P-12 Information Types

NIST SP 800-60 and FIPS 199 assist with identifying the types of information needed to support operating unit missions, business functions, and mission/business processes. Identifying and selecting the appropriate information types is an important step in developing security and privacy minimum security control baseline, security categorization, and SSPP. A list of the needed information types will also assist OPOG and the Cyber Liaisons in determining whether the information system processes PII or BII.

National Archives and Records Administration (NARA) defines the information types that require additional protection as part of the CUI program, following laws, regulations, or government-wide policies. The CSAM application allows operating units to document additional information types that are not identified in NIST SP 800-60 or FIPS 199 to ensure a complete understanding of the types of data being collected, stored, processed, and transmitted by the information system.

4.2.6 RMF Task P-13 Information Life Cycle

The information life cycle describes the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition. Identifying and understanding how each information type is processed during the life cycle helps identify information protection considerations, inform security and privacy risk assessments, and inform control selection and implementation.

4.2.7 RMF Task P-14 Risk Assessment–System

Cybersecurity risk assessment includes identifying threat sources and threat events affecting assets, whether and how the assets are vulnerable to threats, the likelihood that a threat will exploit an asset's vulnerability, and the impact of asset loss. As a key part of the assessment, operating

units should prioritize assets based on the adverse impact or consequence of loss. Interpretations of information loss may include that of possession, destruction, or accuracy.

The loss of a function or service may be that of control or accessibility, ability to deliver normal function, performance, or behavior, or a limited loss of capability resulting in a level of degradation. The compromise's physical consequences can include unscheduled production downtime, equipment damage, casualties at the site, environmental disasters, and public safety threats. Collaborating organizations or mission/business partners prioritize assets based on value, physical consequences, replacement cost, criticality, impact to reputation, and users' trust. The asset priority is the precedence in allocating resources, determining the strength of mechanisms, and defining assurance levels.

The purpose of privacy risk assessments is to determine the likelihood that a given operation the system is taking when processing PII could adversely affect individuals. The following contextual factors influence privacy risk assessments:

- The sensitivity level of the PII, including specific elements or in aggregate
- The types of organizations using or interacting with the system
- Individuals' understanding about the nature and purpose of the processing
- The privacy interests of individuals, technological expertise, or demographic characteristics that influence their understanding or behavior
  Impacts can guide and inform AO decision-making and influence risk response. Risk assessments also determine the potential that using an external provider for the development, implementation, maintenance, management, operation, or disposition of a system, system element, or service could create a loss and the potential impact of that loss

Different assessment processes are:

- Security Risk Assessments - These assessments address the potential adverse impacts to DOC operations, assets, and individuals. Operating units must follow NIST SP 800-30 Rev. 1 for conducting risks assessments on their systems.
- Security Control Assessments - The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system[7]. Operating units must follow the instructions on section 4.6 RMF Step 4 – Assess Security and Privacy Controls.
- Supply Chain Risk Assessment (SCRA) - Operating units must follow the DOC IT Compliance in Acquisition Checklist to determine SCRA requirement applicability and

[7] https://csrc.nist.gov/glossary/term/security_control_assessment

can include information from presumptive awardees, supplier audits, original equipment manufacturers, intelligence sources, etc.

4.2.8 RMF Task P-15 Requirements Definition

SOs must work with relevant stakeholders to define the security and privacy requirements for the system and the environment of operation. Operating units should consider protection needs when defining the requirements for the information system and the environment of operation. Protection needs are an expression of the capability required for the system to reduce risk to an acceptable level while supporting mission or business needs. Protection needs include the security characteristics and the security behavior in its intended operational environment and across all system life cycle phases.

Security and privacy requirements constitute a formal, more granular expression of protection needs across all SDLC phases, the associated life cycle processes, and protections for the assets associated with the system. Security and privacy requirements are obtained from many sources (e.g., laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments). Security and privacy requirements are an important part of the formal expression of the required characteristics of the system. The security and privacy requirements guide and inform the selection of controls for a system and the tailoring activities associated with those controls.

4.2.9 RMF Task P-16 Enterprise Architecture

The security and privacy architectures' primary purpose is to ensure that requirements are consistently and cost-effectively met in DOC systems and align with the risk management strategy. EA is a management practice used to maximize the effectiveness of processes and information resources to achieve mission/business success. An effectively implemented architecture produces more transparent systems that are easier to understand and protect. Enterprise architecture also connects investments to measurable performance improvements.

4.2.10 RMF Task P-17 Requirements Allocation

Allocation of security and privacy requirements guides and informs control selection and implementation for the operating unit, system, system elements, and operation environment. Requirements allocation identifies where to implement controls.

4.2.11 RMF Task P-18 System Registration

To initiate the system registration process, operating units must notify their Cyber Liaison of development plans or system existence, characteristics, and security and privacy implications. System registration provides organizations with a management and tracking tool to facilitate bringing the system into the enterprise architecture, implementing protections that are commensurate with risk, and security and privacy posture reporting following laws, executive orders, directives, regulations, policies, or standards.

Operating units must use the asset tagging capability from BigFix and use the unique CSAM ID sequence number as a primary key for all data analytics and data integration support, including Security Posture Dashboard Report (SPDR), Hardware Asset Management (HWAM), Software Asset Management (SWAM), and other data dashboarding efforts.

4.3 RMF Step 1 – Categorize Information System (System Level)

As part of the system registration process, organizations add the system to the inventory. Upon completion of the Categorization step, the system registration information updates.

In accordance with FIPS 199, operating units must determine security priorities for information systems and apply measures to protect them. The security controls applied to information systems are commensurate with the potential adverse impact on DOC and operating unit operations, organizational assets, individuals, other organizations, and the Nation, should there be a loss of confidentiality, integrity, or availability.

Operating units must complete the FIPS 199 System Categorization using CSAM and NIST SP 800-60, Volumes 1 & 2, and NIST SP 800-122. Operating units must complete this action on the Information Types section in CSAM. The SO must add each applicable information type that is processed, stored, or transmitted by the information system and select the impact level for each security objective. If the system requires an impact level different from the recommended value, the SO must add an explanation detailing why the information system differs.

For unclassified information systems that process PII or BII, OMB Circular A-130 and DOC ECP require the DOC CPO, or their designated representative, to be responsible for reviewing and approving the information system categorization. Potential impact values assigned to security objectives (confidentiality, integrity, availability) must be the highest values from each information type's security determination on the information system. Once operating units detail all information types, CSAM automatically displays each security objective's high watermark.

Operating units can categorize each subsystem if necessary. Separate subsystem categorization does not change the overall categorization. Rather, it allows the subsystems to receive separate and more targeted security and privacy control allocations. This approach is particularly useful when only some subsystems within a system boundary process PII or BII. Interconnections to examine include the interfaces, information flows, and security and privacy dependencies among subsystems and select security and privacy controls.

Operating units should determine whether an increase or decrease in the NIST SP 800-60 provisional security impact levels is necessary based on the system's environment and uniqueness. Changes to the provisional security impact levels must be justified and documented in CSAM.

Table 4-3: Categorize Task Activity List

Task	Activity	Outcome
Task C-1: Information System Description	Document the characteristics of the system	System Description: General and technical description documented in CSAM
Task C-2: System Categorization	Categorize the system and document the security categorization results	Preliminary PII or BII Determination; MOU/MOA/ISA
Task C-3: Categorization Review & Approval	Review and approve the security categorization results and decision	Approval of security categorization for the system

4.3.1 RMF Task C-1 Information System Description

The information system boundary and characteristics information must convey the scope of the system, purpose, high-level requirements, and functionality. This operating unit-level activity occurs in the early phase of the SPA&A process. Operating units must identify and document if the system, or any of its subsystems, manages PII or BII. Operating units should continuously review and update the information system descriptions to ensure it is consistent with the system's purpose and functionality. Operating units must consider the following criteria to determine if the information resources identified as a system fall within the authorization boundary:

- Subject to the same direct management control
- Have the same function or mission objective, operating characteristics, and security needs
- Reside in the same general operating environment
- Manage the same or distinct sets of PII or BII, if applicable
- Adhere to the same security and privacy policies and procedures
- Have the same funding source

Although the above considerations may assist operating units in determining system boundaries for purposes of security and privacy authorization, operating units should not view them as limited flexibility in establishing common-sense boundaries that promote effective security and privacy within the available resources.

For large and complex systems, the AO may examine the feasibility of decomposing the system boundary into subsystems. System and technical descriptions in CSAM must reflect subsystems. Only systems or subsystems that manage PII or BII are required to meet privacy requirements and manage privacy risk before authorization.

4.3.2 RMF Task C-2 System Categorization

The system categorization process analyzes all types of data, known as information types, to determine values for the confidentiality, integrity, and availability of the information system.

4.3.3 RMF Task C-3 System Categorization Review and Approval

OPOG, with recommendations from the operating unit CPO, will review and approve the proposed categorization of information types that include PII or BII. When information systems process PII or BII, the operating unit CPO or their designated representative reviews the information system's selected security categorization. Security categorization results and decisions are reviewed by the AO to ensure that the information system's security category is consistent with and adequately protects mission and business functions. The SO collaborates with operating unit risk management stakeholders to ensure the categorization decision is consistent with the organizational risk management strategy and satisfies high-value assets requirements. As part of the approval process, the AO can provide specific guidance to the SO regarding any limitations on baseline tailoring activities that occur at the RMF Select step. Once the security categorization is approved, the system registration information is updated in CSAM.

4.4 RMF Step 2 – Select Security and Privacy Controls

The NIST SP 800-53B publication establishes security and privacy control baselines for Federal information systems and organizations and provides tailoring guidance for those baselines. The minimum-security control baseline requirements are pre-defined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest.

Table 4-4: Select Task Activity List

Task	Activity	Outcome
Task S-1: Control Selection	Select the controls for the system and the environment of operation	Minimum security control baseline and privacy controls
Task S-2: Control Tailoring	Tailor the controls selected for the system and the environment of operation	Documented justification for updating the minimum impact levels for each information type
Task S-3: Control Allocation	Allocate security and privacy controls to the system and to the environment of operation	CSAM will generate the minimum-security control baseline for the system
Task S-4: Control Documentation	Document the controls for the system and environment of operation in security and privacy plans	Security and privacy plans for the system
Task S-5: Continuous Monitoring Strategy (System)	Develop and implement a system-level strategy for monitoring control effectiveness, consistent with and	Continuous Monitoring Strategy

Task	Activity	Outcome
	supplementing the organizational ISCM Strategy	
Task S-6: Plan Review & Approval	Review and approve the security and privacy plans for the system and the environment of operation	SSPP; Security Requirements Traceability Matrix (SRTM) Report Security and privacy plans approved by the AO

4.4.1 RMF Task S-1 Security and Privacy Control Selection

Operating units must select the initial set of baseline security controls for the information system following FIPS 200 guidance, tailoring the baseline via scoping to remove controls, and supplementing the tailored baseline while considering unique mission and business needs. The initial set of baseline security controls derive from RMF Task 1-3: System Categorization. Upon selection of all the information types in CSAM for the system, the application will automatically import the minimum-security control requirements from NIST SP 800-53B. The privacy risk assessment (*see* Task P-14) and privacy requirements derived from stakeholder protection needs, laws, executive orders, regulations, policies, directives, instructions, and standards (*see* Task P-15) will help inform the selection of privacy controls and privacy control baselines.

4.4.2 RMF Task S-2 Control Tailoring

Upon completion of Task S-1, operating units can tailor the controls based on various factors (e.g., missions or business functions, threats, security, and privacy risks (including supply chain risks), type of system, or risk tolerance). The tailoring of security and privacy control baselines is the foundation for determining the security and privacy controls necessary to protect an information system and is described in detail in SPA&A Appendix E: Security and Privacy Control Tailoring Guide.

4.4.3 RMF Task S-3: Control Allocation

The organization designates controls as system-specific, hybrid, or common (see DOC SCPM), and allocates the controls to the system elements (i.e., machine, physical, or human elements) responsible for providing a security or privacy capability. Controls are allocated to a system or an organization consistent with the organization's enterprise architecture and security or privacy architecture and the allocated security and privacy requirements. Not all controls need to be allocated to every system element. Controls providing a specific security or privacy capability are only allocated to system elements that require that capability. The security categorization, privacy risk assessment, 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.

Additional considerations for control allocation beyond the control baselines must take into account the various control overlays (included in the SPCM) applicable to the information system, interconnection agreements that specify control requirements, financial and financial mixed applications, industry control system implications, and other external threat and risk factors.

The control selection, tailoring, and allocation processes result in a unique set of security control applicability decisions that is specific to the information system based on organizational, operational, and mission needs.

4.4.4 RMF Task S-4 Documentation of Planned Control Implementation

Documentation of security and privacy control implementation allows for traceability of decisions before and after deployment of the information system. The effort required for the implementation statements is commensurate with the purpose, scope, and impact of the system. The security and privacy control implementation description must include any additional information necessary to describe how to achieve the security and privacy capability to support control assessment. Other information systems' control requirements automatically fill into the SSPP with no additional action by the SO.

SSPPs contain an overview of the system's security and privacy requirements, and the controls selected to satisfy the requirements. The plans describe the intended application of each control for the system with detail sufficient to correctly implement the controls and to subsequently assess the effectiveness of the control. The control documentation describes how system-specific, and hybrid controls are implemented and includes the system functionality plans and expectations. The description includes planned inputs, expected behavior, and expected outputs. Security and privacy plans also identify common controls and whether the information system processes PII or BII.

There is no requirement to provide implementation details for program management or common controls in system-level security or privacy plans. For hybrid controls, the operating unit specifies in the system-level plans the parts of the control that are provided by the common control provider.

When developing a consolidated plan, privacy programs collaborate with security programs to ensure that the plan reflects controls that protect the confidentiality, integrity, and availability of PII or BII and delineates roles and responsibilities for control implementation, assessment, and monitoring.

To the extent possible, information systems should reference existing documentation, use automated tools, and coordinate across the organization to reduce redundancy. The documentation also addresses platform dependencies and includes additional information necessary to describe how the capability will be achieved, in enough detail to support control implementation and assessment.

4.4.4.1 Operating Unit Defined Parameters

Once the baseline controls have been appropriately scoped and tailored, the operating unit should define any open parameters in the applicable security and privacy controls. Some controls have parameters prescribed at the Department level and must remain unchanged unless the operating unit wishes to implement more stringent requirements. Security and privacy controls containing operating unit-defined parameters give operating units the flexibility to define certain portions of the controls to support specific requirements.

4.4.4.2 Compensating Controls

Operating units may find it necessary to employ compensating security controls when it is unable to implement a security control in the baseline. The inability may be due to the nature of an information system or its environment of operation. It could also be necessary because the control in the baseline is a cost-ineffective means of obtaining necessary safeguards in place of a recommended baseline security control. Controls must provide an equivalent or comparable level of protection for an information system and the information processed, stored, or transmitted by that system. More than one compensating control may be required to provide the equivalent or comparable protection for particular security controls. Implementing a compensating control occurs under the following conditions:

- The operating unit selects the compensating control from NIST SP 800-53 Rev 5, or if an appropriate compensating control is not available, the organization adopts a suitable compensating control from another source.
- The operating unit provides a supporting rationale for how the compensating control delivers an equivalent security capability for the information system.
- The operating unit assesses and formally accepts the risk associated with employing compensating controls in the information system.

4.4.4.3 Additional Security Control Overlays

Additionally, the operating unit may supplement the tailored baseline with additional security controls or control enhancements to address specific threats to and vulnerabilities within the information system and to satisfy the requirements of applicable federal laws, Executive Orders, directives, policies, standards, or regulations. In many cases, operating units need additional security controls or control enhancements to address specific threats to and vulnerabilities in an information system. Based on the results of the Digital Identity Risk Assessment, or CSAM Threat Matrix Report, operating units may supplement the tailored baseline with additional security controls commensurate with the risk of the information system. Furthermore, operating units may employ gap analysis to identify supplemental controls that address critical threats to the information system. If the operating unit's current security capability or level of preparedness is insufficient, the gap analysis determines the required capability and level of preparedness.

4.4.4.4 Privacy Controls

Privacy controls are administrative, technical, or physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and to manage privacy risks. Privacy risks can include risks beyond those typically included under the confidentiality prong of the information security triad. Operating units shall use privacy controls to manage all privacy risks, regardless of whether those risks would be considered information security risks. To help operating units satisfy privacy requirements and manage privacy risks, NIST developed a set of privacy controls, based on the Fair Information Practice Principles, in NIST SP 800-53 Rev 5. DOC uses the NIST privacy controls to develop its tailored privacy control selection process for information systems. If the operating unit CPO determines that a system does not create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII or BII, the privacy controls should be marked as "N/A" in CSAM.

The DOC CPO is responsible for designating which privacy controls DOC treats as program management, common, information system-specific, and hybrid. Privacy program management controls are controls that are generally implemented at the operating unit level and essential for managing the DOC's privacy program.

When the operating unit assigns privacy controls to an information system as information system-specific, hybrid, or common controls, they assign responsibility and accountability to specific operating unit programs or officials for the overall development, implementation, assessment, authorization, and monitoring of those controls. In all cases, the DOC CPO must maintain oversight and coordinate privacy control management.

4.4.5 RMF Task S-5 System Continuous Monitoring Strategy

A critical aspect of risk management is the ongoing monitoring of security and privacy controls employed within or inherited by the information system. DOC implements a continuous monitoring program that allows an operating unit near real-time visibility into the system's security posture utilizing CSAM and ECDM.

This program allows risk monitoring and management of the information system over time. It also maintains the initial authorization in a dynamic operational environment with changing threats, vulnerabilities, technologies, and missions/business functions. The DOC's continuous monitoring program includes configuration management and control processes at the system-specific level; security and privacy impact analyses on proposed or actual changes to the information system and its environment of operation; assessment of selected security and privacy controls employed within and inherited by the information system; and security and privacy status reporting to appropriate stakeholders.

4.4.6 RMF Task S-6 Plan Review and Approval

Once the operating unit completes the previous tasks, the Information System Security Officer (ISSO) must generate the SSPP and SRTM Report using the CSAM report function.

The SRTM contains the security controls selected to satisfy DOC cybersecurity requirements for the information system. The SSPP contains the system categorization and the SSPP Agreement Summary that must be signed to indicate approval. The SSPP also contains whether the information system manages PII or BII and the proposed privacy controls to address privacy risks and ensure compliance with applicable privacy requirements. As a result, the AO agrees to the set of security and privacy controls proposed to meet the information system's risk requirements. The approval of the SSPP also establishes the effort required to complete the remaining steps in the RMF/CSF. Additionally, it provides the basis of the specification to acquire the information system, subsystems, or operating units.

After all required stakeholders, including operating unit CPO, review and approve the SSPP it becomes an approved artifact in CSAM.

4.5 RMF Step 3 – Implement Security and Privacy Controls

An operating unit must implement the controls as described in the SSPP. Operating units must consider the security impact level of the information system when implementing controls, including systems security and privacy concerns. Operating units must apply the DOC minimum defined parameters documented in the SPCM and establish operating unit and system level control parameters based upon mission and business need. Operating units must follow privacy requirements and adhere to privacy compliance processes as established by the DOC OPOG and DOC CPO.

Table 4-5: Implementation Task Activity List

Task	Activity	Outcome
Task I-1: Control Implementation	Implement the controls in the SSPP	Document the implementation of security controls
Task I-2: Update Control Implementation Information	Document changes to planned control implementations based on the "as-implemented" state of controls	SSPP; Incident Response Management Standard[8]; Contingency Plan Standard[9]; Configuration Management Plan Standard[10]

4.5.1 RMF Task I-1 Control Implementation

Operating units must adhere to the DOC SPCM when implementing the minimum security and privacy controls. This Handbook ensures a consistent approach to building security and privacy

[8] Find Incident Response Management Standard at Enterprise Cybersecurity Policy Program | Commerce Connection

[9] Find Contingency Plan Standard at Enterprise Cybersecurity Policy Program | Commerce Connection

[10] Find Configuration Management Standard at Enterprise Cybersecurity Policy Program | Commerce Connection

into the acquisition, development, and deployment of information systems. Operating units must satisfy minimum assurance requirements to be confident that controls are implemented correctly, operating as intended, and producing the desired outcome. At this point in the system development, assurance requirements are imposed on the system developers to address the quality of the design, development, and implementation of the security and privacy functions.

When operating units cannot fully implement controls, they may need to employ compensating controls that provide equivalent or comparable protection for an information system. The use of compensating controls must be documented in the SSPP. If an operating unit intends to use a compensating privacy control(s), the operating unit CPO and associate privacy officer (APO) or authorized representative must approve.

4.5.2 RMF Task I-2 Update Control Implementation Information

Despite the control implementation details in the security and privacy plans and the system design documents, it is not always feasible to implement controls as planned. Therefore, as control implementations are carried out, the security and privacy plans are updated with as-implemented control implementation details.

The Determine If Statements are the control requirements along with the organizational defined values (or system specific) for each control. Determine If Statements that are fully inherited will not require documentation or later assessment by the SO. However, the SO must address Determine If Statements that are hybrid in the implementation statement of the control. At this phase in the development of the system, operating units must develop the Incident Response Plan (IRP), Contingency Plan (CP), Configuration Management Plan (CMP), and Privacy documents.

4.6 RMF Step 4 – Assess Security and Privacy Controls

The AO has the flexibility to consider both the technical expertise and level of independence necessary to successfully execute information system security control assessments. Security and privacy control assessments must be performed by resources with the necessary skills and technical expertise to develop effective assessment plans and to conduct assessments of program management, system-specific, hybrid, and common controls, as appropriate.

Table 4-6: Assessment Task Activity List

Task	Activity	Outcome
Task A-1: Assessor Selection	Select the appropriate assessor or assessment team for the type of control assessment to be conducted	None
Task A-2: Assessment Plan	Develop, review, and approve plans to assess implemented controls	Security and Privacy Assessment Plan
Task A-3: Control Assessments	Assess the controls in accordance with the procedures described in assessment plans	None

Task	Activity	Outcome
Task A-4: Assessment Reports	Prepare the reports documenting the findings and recommendations from the control assessments	Security and Privacy Assessment Report
Task A-5: Remediation Actions	Conduct initial remediation actions on the controls and reassess remediated controls	Updated SSPP, Updated SPAR
Task A-6: Plan of Action & Milestones	Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports	POA&M Report

4.6.1 RMF Task A-1 Assessor Selection

AO's must consider technical expertise and independence levels when selecting control assessors to develop effective assessment plans and conduct assessments. Operating units can conduct self-assessments or obtain an independent control assessor that can conduct an impartial assessment. Impartiality means that assessors are free from perceived or actual conflicts of interest regarding control effectiveness determination or the development, operation, or management of the system, common controls, or program management controls.

The AO determines the level of assessor independence based on applicable laws, executive orders, directives, regulations, policies, or standards. When the SCA is not required by the AO to be independent, an AO must review the SSPP, SPAR, and all POA&Ms provided by the SCA and sign the Authorization memorandum.

The DOC CPO is responsible for conducting assessments of privacy controls and documenting the results of the assessments. At the discretion of the organization, privacy controls may be assessed by an independent assessor. However, the DOC CPO is responsible and accountable for the organization's privacy program, including any privacy functions performed by independent assessors. When an information system processes PII or BII, the operating unit CPO is responsible for identifying assessment methodologies and metrics to determine if privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks.

4.6.2 RMF Task A-2 Assessment Plan

The security and privacy control test plan provides assessment objectives, a detailed process, and procedures that reflect the method of assessment the operating unit is conducting. In conjunction with the operating unit CPO, operating units should work to develop a comprehensive plan to assess the security and privacy controls employed within the information system for each control assessment.

4.6.3 RMF Task A-3 Control Assessments

Security control assessments determine whether controls are correctly implemented, operating as intended, and producing the desired outcome of meeting the information system's requirements. From a security perspective, the objective is to identify the cybersecurity architecture and security controls to ensure that the system design and testing validate the implementation. Privacy control assessments determine whether the controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage risks.

4.6.4 RMF Task A-4 Assessment Reports

The SPAR contains the results of the control assessment and is an essential factor in an AO's determination of risk to operating unit operations, assets, individuals, other organizations, and the Nation. The Security Control Assessor (SCA) or the Privacy Control Assessor (PCA) may supplement the SPAR with additional documentation if the SO or AO request it. Operating units must ensure all CSAM required inputs, including the dates on the Status screen, reflect the most current SPAR.

4.6.5 RMF Task A-5 Remediation Actions

Remediation actions are essential to addressing weaknesses and deficiencies in the information system and its operational environment based on the SPAR findings. Operating units must review identified weaknesses and deficiencies to determine the severity or criticality of the findings and potential adverse impacts on operating unit assets, and whether certain findings are significant to require immediate remediation.

Identified weaknesses that could not be resolved during a security control assessment will have up to 30 calendar days from the SPAR publication for POA&M creation. If weaknesses or deficiencies in security or privacy controls are corrected, operating units must reassess the remediated controls for effectiveness and document the current assessment results.

The operating unit must update the SSPP based on the SPAR results and any subsequent changes to the information system so that the SSPP reflects an accurate list and description of the controls implemented. Operating units must also generate an updated SPAR.

4.6.6 RMF Task A-6 Plan of Action and Milestones

POA&Ms describe plans for specific tasks to correct any deficiencies in the security and privacy controls identified during the assessment. POA&Ms also include a recommendation for completion before or after system authorization, resources required to accomplish the tasks, milestones established to meet the tasks, and the scheduled completion dates for the milestones and task. They also address the residual vulnerabilities in the information system. For information systems that manage PII or BII, privacy controls selected may relate to specific legal requirements. The DOC CPO must review and approve a POA&M for a privacy control that is selected to ensure compliance with statutory, regulatory, or Executive Branch policy requirements.

4.7 RMF Step 5 – Authorize Information System

Authorization packages include security and privacy plans, assessment reports, POA&Ms, and an executive summary. Additional information can be included in the authorization package at the request of the AO. Operating units maintain version and change control in CSAM as the information in the authorization package is updated. Providing timely updates to the plans, assessment reports, and POA&Ms on an ongoing basis supports the concept of near real-time risk.

Since the DOC CPO is designated by the head of each agency, input and recommendations submitted by the DOC CPO must be considered in the authorization decision. The DOC CPO reviews the authorization package for information systems that process PII or BII to ensure compliance with applicable privacy requirements and to manage privacy risks, prior to AOs making risk determination and acceptance decisions. In situations where the AO and the DOC SAOP cannot reach a final resolution regarding the appropriate protection for the agency information and information system, the head of the agency must review the associated risks and requirements and make a final determination regarding the issuance of the ATO.

When controls are implemented by an external provider through contracts, interagency agreements, lines of business arrangements, licensing agreements, or supply chain arrangements, the operating unit ensures that the information needed to make risk-based decisions is made available by the provider. DOC uses CSAM as an automated tool to support in preparing and managing the content of the authorization package. The authorization documents are updated when there is a system change, incident impacting system operations, or during system reauthorization.

Table 4-7: Authorization Task Activity List

Task	Activity	Outcome
Task R-1: Authorization Package	Assemble the authorization package and submit the package to the AO for a decision	Security and Privacy Authorization Package
Task R-2: Risk Analysis & Determination	Analyze and determine the risk from the operation or use of the system or the provision of common controls	Risk Determination
Task R-3: Risk Response	Identify and implement a preferred course of action in response to the risk determined	Risk Responses for determined risks
Task R-4: Authorization Decisions	Determine if the risk from the operation or use of the system, the provision, or common controls is acceptable	ATO, Authorization to Use (ATU), Denial of ATO (DATO)
Task R-5: Authorization Reporting	Report the authorization decision and any deficiencies that	A report indicating the authorization decision or set of common controls;

Task	Activity	Outcome
	represent significant security or privacy risk	annotation of status in the system registry

4.7.1 RMF Task R-1 Authorization Package

The authorization package provides the AO with the essential information necessary to decide whether to grant an ATO. The package must contain the SSPP, SPAR, and POA&Ms with an executive briefing summarizing the high-level information about the system.

If the information system processes PII or BII, an AO shall review the SSPP, SPAR, and all POA&Ms provided by the PCA.

4.7.2 RMF Task R-2 Risk Analysis and Determination

The Information SO, along with the operating unit CPO when the information system processes PII or BII, must brief or provide the AO with information on the system's current security and privacy state and the recommendations for addressing any residual risks. The SPAR is employed to provide necessary information on threats, vulnerabilities, privacy risks, and potential impacts and the analyses for the risk mitigation recommendations.

4.7.3 RMF Task R-3 Risk Response

After risk is analyzed and determined, organizations can respond to risk in various ways, including risk acceptance or mitigation. When the response to risk is mitigation, the planned actions are included in and tracked using POA&Ms. Once mitigated, assessors reassess the controls to determine the extent to which remediated controls are implemented correctly, operating as intended, and producing the desired outcome. The assessors update the reports with the reassessment findings and document the current assessment results. The SSPP is updated based on the findings of the control assessments and any remediation actions taken. The updated SSPP reflects the state of the controls after the initial assessment and any modifications by the SO or common control provider in addressing recommendations for corrective actions.

After completing security and privacy control reassessments, the SSPP contains an accurate description of implemented controls, including compensating controls. When the response to risk is acceptance, the deficiencies found during the assessment process are documented in the SPAR and monitored for changes to the risk factors.

The AO is responsible for reviewing the assessment reports, POA&Ms, and, if applicable, the Risk Acceptance Memo to determine whether to mitigate identified risks before authorization.

Decisions on the most appropriate course of action for responding to risk may include some form of prioritization. Some risks may be of greater concern to organizations than other risks. Prioritizing risk response does not mean ignoring lower-priority risks. A key part of the risk-based decision process is the recognition that regardless of the risk response, there remains a degree of

residual risk. Operating units determine acceptable degrees of residual risk based on organizational risk tolerance.

4.7.4 RMF Task R-4 Authorization Decisions

The AO must be able to determine the risk to organizational operations and assets, individuals, other organizations, and the Nation and the appropriateness of such risk given the mission or business needs. The AO must weigh the relevant factors and request to accept or reject the risk to their operating unit and DOC in an authorization memorandum. Changes in an AO require the incoming AO to sign a new authorization decision document within 180 days of assignment, thus formally transferring responsibility and accountability for the information system. In alignment with NIST SP 800-37 Rev. 2, DOC recognizes the following types of authorization decisions:

Authorization to Operate: The AO deems the risk to the DOC, operating unit operations, assets, and individuals acceptable. The ATO duration cannot exceed three years unless the information system is entering into the DOC Ongoing Authorization (OA) status.

Authorization to Use: The AO may issue an Authorization to Use (ATU) depending on an operating unit's unique mission or business requirements. An ATU is employed when an organization (hereafter referred to as the customer organization) chooses to accept the information in an existing authorization package produced by another organization (either federal or nonfederal) for an information system that is authorized to operate by a federal entity (referred to as the provider organization). The introduction of NIST SP 800-37 Rev. 2 promotes this type of authorization. The issuance of an ATU does not reduce or eliminate the level of risk management responsibility and authority of the AO. The ATU process allows the operating unit to streamline and perform more security control tailoring based upon business needs. Like with an ATO, an ATU cannot be issued for information systems that process PII or BII without the operating unit CPO or APO reviewing the authorization package and signoff by the DOC SAOP. In lieu of issuing an ATO, the AO will issue a risk-based decision indicating explicit acceptance of the security and privacy risk incurred from the use of a shared system, service, or application with respect to the information processed, stored, or transmitted by or through the shared or cloud system, service, or application.

Common Control Authorization: A common control authorization is similar to an ATO for systems. If the AO, after reviewing the authorization package submitted by the common control provider, determines that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable, a common control authorization is issued. It is the responsibility of common control providers to indicate that the common controls selected by the organization have been implemented, assessed, and authorized and are available for inheritance by organizational systems. Common control providers are also responsible for ensuring that the SOs inheriting the controls have access to appropriate documentation and tools.

Common controls are authorized for a specific time period in accordance with the terms and conditions established by the AO and the organization. An authorization termination date is

established by the AO as a condition of the initial common control authorization. The termination date can be adjusted at any time to reflect the level of concern by the AO regarding the security and privacy posture of the common controls that are available for inheritance. If the controls are under ongoing authorization, a time-driven authorization frequency is specified. Within any authorization type, an adverse event could trigger the need to review the common control authorization. Common controls that are implemented in a system do not require a separate common control authorization because the controls receive an ATO as part of the system ATO.

The CSAM application allows for two implementations of a type of authorization:

1. The first option is to establish an inventory item for the archetype aspects of the system and to establish subsystem inventory items for each deployed instance to address the deployment-specific aspects. This method allows for greater flexibility in assigning specific users or groups' access to their deployment-specific information within CSAM. DOC recommends this option for a larger number of deployments, or those deployments to different groups or management structures who wish to keep assessment information within their purview.
2. The second option is to utilize a single inventory item representing all deployments of the information system. DOC recommends this option with a limited number of deployments and strong central management, including the resources to assess each deployment's compliance with the required security and privacy controls in the single inventory item. This form of authorization allows for a single authorization package (i.e., SSPP, SPAR, POA&M) and centralized risk reporting, which leads to a better organizational view of the system deployment risks.

Type assessment procedures are the same until the authorization step. Each deployment of a system utilizing a type of authorization must assess the deployment-specific controls before authorization and operation. When the system is authorized, there are two authorization techniques available. The first is to utilize a single ATO for the archetype and deployments. The second is to utilize a central ATO for the archetype and additional Authorizations to Operate for the deployments.

When the operating unit has no implementation or testing responsibility, DOC only requires the documentation review described above and a memo. The memo is from the SO to the AO, signed by both, indicating that the operating unit is leveraging the ATO from another department or agency and that it meets minimum assurance standards. On an annual basis, the operating unit must request updated documentation to ensure continued compliance with all necessary laws, regulations, and policies.

If an operating unit utilizes an external information system for which the operating unit has some control over implementation and testing responsibility, the appropriate implementation and test methodology and result statements must be entered into CSAM. Enter this information utilizing the SPA&A process above, noting externally inherited controls as provided by the owning department or agency.

Denial of Authorization to Operate: If the AO deems that the risk is unacceptable, they deny the ATO, and the system will not be operational. If the system is currently in operation, all activity should halt, and the system should be removed from the operational network.

4.7.5 Ongoing Authorization

The DOC OA framework provides direction for the transition to continuous authorization from the standard three-year ATO cycle for all supporting information systems. The OA is applicable to all DOC information systems (unclassified and classified) including contractor-operated systems and externally operated systems that collect, store, process, or transmit DOC information. Operating unit policy supplementation, including any policies or procedures that are more stringent, must be mission- and risk-based. Any deviations that do not meet the minimum requirements from this standard in conducting the security and privacy assessment and continuous authorization shall follow the DOC OCRM cybersecurity policy waiver process and be coordinated through OCRM and approved by the DOC CPO and DOC CIO before information systems can be granted or maintain continuous authorization. Information systems transitioning to OA must have an official ATO memorandum authorized by the operating unit AO and submitted to the DOC CPO and DOC CISO for approval.

A robust continuous monitoring program provides the AO and stakeholders a holistic view of the vulnerabilities and risk inherent in the operations of the system and guides the decision for continuous operation of the system. It is also closely related to the dynamic, DOC-wide risk management process that develops a more refined and articulate situational awareness of an organization's security and risk posture based on the ongoing assessment, response to, and monitoring of information security risk.

Reauthorizations are unnecessary when an information system transitions from a static, point-in-time authorization to a dynamic, near real-time OA process. For information systems to enter into OA, operating units must meet the following conditions:

- The system or common control(s) has received an initial authorization, and the information system integrates all RMF Steps into the system development life cycle and effectively applies the DOC's ISCM Handbook.
- The information system stakeholder(s) monitors implemented controls with the appropriate degree of rigor and at the required frequencies specified in the DOC ISCM Handbook.
- The continuous security and privacy documentation generated provides the AO and other stakeholders visibility and awareness through security and privacy management and reporting tools such as CSAM. Such tools facilitate risk-based decision making for the OA for systems and common controls.
- There are no significant changes to the information system controls, operations, and introduction of major security risk through system compromise.
- The system authorization boundary is clearly defined, assets are tagged with the authorization boundary ID, and each asset uses Continuous Diagnostics and Mitigation

(CDM) and other enterprise security tools. If an enterprise security tool is not used, the system must record, as an OA artifact, an approved waiver to deviate from the enterprise security tool.

For guidance on HVA systems in ongoing authorization, refer to the HVA Handbook[11].

4.7.6 RMF Task R-5 Authorization Reporting

AOs report authorization decisions for systems and common controls to designated organizational officials. The designated officials view the individual risk decisions in the context of DOC-wide security and privacy risk to organizational operations and assets, individuals, other organizations, and the Nation. Reporting occurs only in situations where organizations have delegated the authorization functions to levels below the head of the agency. AOs also report exploitable deficiencies in the system or controls noted during the assessment and continuous monitoring that represent significant security or privacy risk. Operating units determine, and the organizational policy reflects, what constitutes significant security or privacy risks to report. Deficiencies that represent significant vulnerabilities and risks are reportable using the Subcategories, Categories, and Functions in the NIST CSF.

4.8 RMF Step 6 – Monitor Security and Privacy Controls

DOC system operations are in a constant state of change with changes occurring in the technology, human elements, and physical or environmental elements. System changes include changes to the technology, upgrades to hardware, software, or firmware; changes to the human elements, staff turnover or a reduction in force; and modifications to the surrounding physical and environmental elements, location or the physical access controls protecting the facility. Changes made by external providers can be difficult to detect. A disciplined and structured approach to managing and documenting changes to systems and environments of operation, and adherence with terms and conditions of the authorization, is an essential element of security and privacy programs.

Operating units must monitor for unauthorized changes, which may occur because of purposeful attacks by adversaries or inadvertent errors by authorized personnel. In addition to adhering to the established DOC CM Standard, operating units shall monitor for unauthorized changes to systems and analyze information about the changes that have occurred to determine the root cause.

[11] Find High Value Assets Handbook at Enterprise Cybersecurity Policy Program | Commerce Connection.

Table 4-8: Control Monitoring Activity List

Task	Activity	Outcome
Task M-1: System and Environmental Changes	Monitor the information system and its environment of operation for changes that impact the system's security and privacy posture	Security and Privacy Impact Analyses
Task M-2: Ongoing Assessments	Assess the controls implemented within and inherited by the system in accordance with the ISCM Strategy	Security and Privacy Assessment Report Analysis
Task M-3: Ongoing Risk Response	Respond to risk based on results of ongoing monitoring activities, risk assessments, & outstanding items in POA&Ms	Updated POA&M Report
Task M-4: Authorization Package Updates	Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process	SSPP; SPAR; Residual Risk Report; MOU/MOA; ISA; CP; IRP; CMP
Task M-5: Security and Privacy Reporting	Report the security and privacy posture of the system to the AO & other organizational officials on an ongoing basis per the DOC ISCM Strategy	Security and Privacy Status Reports
Task M-6: Ongoing Authorization	Review the security and privacy posture of the system on an ongoing basis to determine if the risk remains acceptable	Updated Authorization Package; Updated Authorization Memos
Task M-7: System Disposal	Implement a system disposal strategy and execute required actions when a system is removed	System Decommissioning Plan; System Retirement Memo

4.8.1 RMF Task M-1 System and Environmental Changes

Information systems are constantly changing with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and operate. The change management process requires the submission of change requests, completion of security

and privacy impact analyses, and the processing, approval or disapproval, and implementation of all approved changes.

Operating units must maintain strict configuration management and control processes to support ISCM activities. It is important to record any relevant information about specific hardware, software, or firmware changes such as version or release number, 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, including modifications to hosting networks and facilities, mission/business use of the system, and threats.

Operating units must initiate a security and privacy impact analysis to determine the extent to which proposed changes to the information system, or its operating environment may affect or have affected the system's ATO. If someone other than the operating unit CPO is responsible for completing the privacy impact analysis, the operating unit CPO, or their designated representative, is responsible for reviewing the analysis to determine whether the proposed change affects the privacy state of the system. If the results of the security and privacy impact analysis indicate that the proposed change can affect the security or privacy state of the system, operating units must initiate corrective actions and revise documentation, including the SSPP, SPAR, and POA&Ms.

4.8.2 RMF Task M-2 Ongoing Assessments

Operating units must assess all security and privacy controls selected for the information system during the initial authorization and any subset of the security or privacy controls during continuous monitoring on an ongoing basis. Annual security and privacy control selection is comprised of Core Controls described in the DOC SPCM and any requirements falling within that year, OMB A-123 controls, controls associated with POA&Ms closed within the last 12 months, and any operating unit-selected controls for the current fiscal year. Each system not undergoing an initial authorization must undergo an annual assessment for continuous monitoring activities. The three selections identified above represent the controls to assess, at least during the annual assessment.

Operating units must assess all controls associated with POA&Ms closed within the previous 12 months to ensure remediation actions' successful implementation. Operating units must also assess all OMB A-123 controls if applicable.

4.8.3 RMF Task M-3 Ongoing Risk Response

As part of the overall DOC ISCM strategy, it is critical that operating units actively remediate control deficiencies. Operating units must update the assessment of the security and privacy controls in accordance with DOC's Core Control assessment schedule.

A POA&M closure requires testing of the corrective action and update to the SSPP. Operating units must create POA&Ms for all deficiencies, regardless of source, that they cannot remediate within 30 days.

4.8.4 RMF Task M-4 Authorization Package Updates

To facilitate the near real-time management of risk associated with the operation and use of the information system, the operating unit must update all documentation related to the SPA&A process to reflect any changes that have occurred, as necessary and appropriate. Using CSAM, operating units must monitor and update all required inputs to ensure that they reflect the above documentation's most recent updates.

4.8.5 RMF Task M-5 Security and Privacy Reporting

Security and privacy status reports provide the AO and other senior operating unit leaders with essential information about the information system's security and privacy state and operating environment. Security status reports must be provided to system stakeholders at least monthly. At a minimum, the security status report should include details on the information system's security posture, major risks or vulnerabilities, POA&Ms status, and key authorization activities.

4.8.6 RMF Task M-6 Ongoing Authorization

During this task, the AO reviews the information system's reported security and privacy status periodically to determine the current risk to operating unit operations and assets, individuals, other organizations, and the Nation. The AO must determine whether the current risk is acceptable and provide appropriate direction to the Information SO. The risks incurred may change over time based on the information provided in the security and privacy status reports. Based on the ongoing risk determinations, including major modifications, expanded collection or use of PII, BII, or law, directive, policy, or regulation updates, the AO may require a formal, independent reauthorization assessment to be conducted.

4.8.7 RMF Task M-7 System Disposal

While retired information systems have effectively reached the final phase in the system development life cycle, operating units must retain system documentation for audit purposes. Disposal activities ensure the orderly termination of the system and preservation of vital information in the event an operating unit may need to reestablish the system in the future. During any retirement activities, the operating unit must ensure the implementation of all security controls that address information system removal and decommissioning. The operating unit must also ensure the implementation of all privacy controls addressing the disposition and retention of PII or BII. Operating units must update tracking and management systems to indicate the specific information system operating units removed from service. Security and privacy status reports must reflect the new status of the information system. Any security or privacy control inheritance relationships must be reviewed and assessed for impact.

5 Cloud Service Provider Assessment Requirements

The shift to cloud computing necessitates adjustments to the DOC risk management process, which typically address physical on-premises systems and applications, to accommodate the use of Cloud Service Providers (CSPs) and their Cloud Service Offerings (CSOs). CSPs offer three cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

- **SaaS:** The capability provided to a DOC operating unit is to use the CSP applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. A DOC operating unit does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user-specific application configuration settings.
- **PaaS:** The capability provided to a DOC operating unit is to deploy onto the cloud infrastructure mission owner-created or acquired applications created using programming languages, libraries, services, and tools supported by the CSP. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. A DOC operating unit does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- **IaaS:** The capability provided to a DOC operating unit is to provision processing, storage, networks, and other fundamental computing resources where a mission owner can deploy and run arbitrary software, which can include operating systems and applications. A DOC operating unit does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking operating units (e.g., host firewalls).

A key element to successful adoption of cloud services is to ensure that essential security controls are properly implemented, and that effective security management based on risk management and compliance is applied. Operating units are required to follow requirements established in the FedRAMP Agency Authorization Playbook [12] and SPA&A Appendix G: Cloud Service Provider Assessment Guide for systems within their scope[13].

[12] https://www.fedramp.gov/assets/resources/documents/Agency_Authorization_Playbook.pdf

[13] https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf

Appendix A: Acronyms

Acronym	Definition
AO	Authorizing Official
APO	Associate Privacy Officer
ATO	Authority to Operate
ATT	Authority to Test
ATU	Authorization to Use
BII	Business Identifiable Information
BOD	Binding Operational Directives
CCP	Common Control Program
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CM	Configuration Management
CMP	Configuration Management Plan
CNSS	Committee on National Security System
CNSSP	Committee on National Security System Policy
CP	Contingency Plan
CPO	Chief Privacy Officer
CSAM	Cyber Security Assessment and Management
CSF	NIST Cybersecurity Framework
CSO	Cloud Service Offerings
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
Department or DOC	Department of Commerce
DHS	Department of Homeland Security
DoD	Department of Defense

Acronym	Definition
EA	Enterprise Architecture
ECDM	Enterprise Continuous Diagnostics and Monitoring
ECP	Enterprise Cybersecurity Policy
ED	Emergency Directives
FEAF	Federal Enterprise Architecture Framework
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
HVA	High Value Asset
HWAM	Hardware Asset Management
IaaS	Infrastructure as a Service
IC	Intelligence Community
ICD	Intelligence Community Directives
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
MES	Mission Essential System
MOU/A	Memorandum of Understanding/Agreement
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OA	Ongoing Authorization
OCIO	Office of the Chief Information Officer
OCRM	Office of Cybersecurity and IT Risk Management
OIG	Office of Inspector General
OMB	Office of Management and Budget

Acronym	Definition
OPOG	Office of Privacy and Open Government
PaaS	Platform as a Service
PCA	Privacy Control Assessor
PII	Personally Identifiable Information
PO	Privacy Officer
POA&M	Plan of Action & Milestones
RMF	Risk Management Framework
SaaS	Software as a Service
SAOP	Senior Agency Official for Privacy
SPAR	Security and Privacy Assessment Report
SCA	Security Control Assessor
SCRA	Supply Chain Risk Assessment
SCRM	Supply Chain Risk Management
SDLC	System Development Lifecycle
SPDR	Security Posture Dashboard Report
SWAM	Software Asset Management
SO	System Owner
SP	Special Publication
SPA&A	Security and Privacy Assessment & Authorization
SPCM	Security and Privacy Controls Matrix
SRTM	Security Requirements Traceability Matrix
SSPP	System Security and Privacy Plan

Appendix B: Glossary

Term	Definition
Agency	Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.
Allocation	The process an organization employs to determine whether security controls are defined as system-specific, hybrid, or common. The process an organization employs to assign security controls to specific information system operating units responsible for providing a particular security capability.
Application	A software program hosted by an information system.
Assessment	See control assessment or risk assessment.
Assessment Plan	The objectives for the control assessments and a detailed roadmap of how to conduct such assessments.
Assessor	The individual, group, or organization responsible for conducting a security or privacy assessment.
Assurance	The grounds for confidence that the set of intended controls in an information system are effective in their application.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted, confidence in the validity of a transmission, a message, or message originator.
Authorization (to operate)	The official management decision given by a senior Federal official(s) to authorize operation of an information system and accept the risk to agency operations, agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls.
Authorization (to use)	The official management decision given by an authorizing official to authorize the use of an information system, service, or application based on the information in an existing authorization package generated by another organization, and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of controls in the system, service, or application.
Authorization Boundary	All operating units of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems to which the system is connected.

Term	Definition
Authorization Package	The essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the use of a designated set of common controls.
Authorizing Official	A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.
Authorizing Official Designated Representative	An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with the authorization process.
Availability	Ensuring timely and reliable access to and use of information.
Baseline	The set of controls that are applicable to information or an information system to meet legal, regulatory, or policy requirements, as well as address protection needs for the purpose of managing risk.
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, using boundary protection devices.
Boundary Protection Device	A device with appropriate mechanisms that facilitates the adjudication of different interconnected system security policies and/or provides information system boundary protection.
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where a person other than an authorized user accesses or potentially accesses PII/BII or an authorized user accesses or potentially accesses PII/BII for an other-than-authorized purpose. It includes both external intrusions and internal misuse.
Business Identifiable Information	Information that is defined in the FOIA as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." This information is not confined to records that reveal "basic commercial operations," but also includes any records or information in which the submitter has a "commercial interest" and can include information submitted by a nonprofit entity; or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C. 9).
Capability	A combination of mutually reinforcing controls implemented by technical means, physical means, and procedural means. Such controls are typically selected to achieve a common information security or privacy purpose.
Classified Information	Information that has been determined to be pursuant to Executive Order 13526, or any predecessor Order, to be classified national security information; or pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data.

Term	Definition
Common Control	A control that is inherited by one or more organizational information systems.
Common Control Provider	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls.
Compensating Controls	The management, operational, and technical controls employed by an organization in lieu of the recommended controls in the baselines described in NIST SP 800-53 Rev 5 and CNSS Instruction 1253, that provide equivalent or comparable protection for an information system.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Configuration Settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.
Continuous Monitoring	The process implemented to maintain a current security and/or privacy status for one or more information systems or for the entire suite of information systems on which the operational mission depends.
Continuous Monitoring Program	A program established to collect information in accordance with preestablished metrics, utilizing information readily available in part through implemented security controls.
Control Effectiveness	A program established to collect information in accordance with preestablished metrics, utilizing information readily available in part through implemented security controls.
Controlled Unclassified Information	Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.
Countermeasure	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Cybersecurity Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.

Term	Definition
Cybersecurity Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access resources as defined by a common security policy, security model, or security architecture.
Environment of Operation	The physical surroundings in which an information system processes, stores, and transmits information.
Event	Any observable occurrence in a network or information system.
Federal Enterprise Architecture	A business-based framework for government-wide improvement that intends to transform the federal government to be citizen-centered, results-oriented, and market-based.
High Value Asset	Those assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people.
Hybrid Control	A control that is implemented in an information system in part as a common control and in part as a system-specific control.
Incident	An occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form.
Information Life Cycle	The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.
Information Resources	Information and related resources, such as personnel, equipment, funds, and technology.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior of the enterprise security processes, information security systems,

Term	Definition
	personnel, and organizational subunits, showing their alignment with the enterprise's mission and strategic plans.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information Technology	Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.
Information Type	A specific category of information defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Interface	A connection outside of the security authorization boundary; a dedicated connection between information systems which does not apply to transitory, user-controlled connections such as email and website browsing.
Management Controls	The safeguards or countermeasures for an information system that focus on the management of risk and the management of information system security.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
National Security System	Any information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications); or is protected at all times by procedures specifically authorized to be kept classified in the interest of national defense or foreign policy.
Network	Information system(s) implemented with a collection of interconnected operating units. Such operating units may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

Term	Definition
Object	Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object (by a subject) implies access to the information it contains.
Ongoing Authorization	The risk determinations and risk acceptance decisions subsequent to the initial authorization, taken at agreed-upon and documented frequencies in accordance with the agency's mission or business requirements and agency risk tolerance. Ongoing authorization is a time-driven or event-driven authorization process whereby the authorizing official is provided with the necessary and sufficient information regarding the security and privacy state of the information system to determine whether the mission or business risk of continued system operation is acceptable.
Organization	An entity of any size, complexity, or positioning within an organizational structure.
Overlay	A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact	The loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect (FIPS 199 low); a *serious* adverse effect (FIPS 199 moderate); or a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Privacy Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's privacy protection processes, technical measures, personnel, and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.
Privacy Control	The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.
Privacy Control Assessment	The testing and/or evaluation of the privacy controls in an information system that creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of PII/BII to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the privacy requirements for the system.
Privacy Control Inheritance	A situation in which an information system or application receives protection from privacy controls (or portions of privacy controls) that are developed, implemented,

Term	Definition
	assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *Common Control.*
Privacy Plan	A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.
Privacy Posture	The privacy posture represents the status of the information systems and information resources (e.g., personnel, equipment, funds, and information technology) within an organization based on information assurance resources (e.g., people, hardware, software, policies, procedures) and the capabilities in place to comply with applicable privacy requirements and manage privacy risks and to react as the situation changes.
Privacy Requirement	A requirement that applies to an information system or an organization that is derived from applicable laws, executive orders, directives, policies, standards, regulations, procedures, and/or mission/business needs with respect to privacy.
Reauthorization	The risk determination and risk acceptance decision that occurs after an initial authorization.
Records	All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. [44 U.S.C. § 3301] (Note: Unless otherwise stated, this definition is distinct from "records" as defined under the Privacy Act of 1974. 5 U.S.C. § 552a)
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of the adverse impact, or magnitude of harm that would arise if the circumstance or event occurs, and the likelihood of occurrence.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system
Risk Executive	An individual or group within an organization, led by the senior accountable official for risk management, that helps to ensure that security risk considerations for individual systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and managing risk from individual systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

Term	Definition
Risk Management	The program and supporting processes to manage risk to agency operations, agency assets, individuals, other organizations, and the Nation,
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk reducing controls/countermeasures recommended from the risk management process.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to agency operations, agency assets, individuals, other organizations, or the Nation.
Safeguards	Protective measures prescribed to meet the security requirements specified for an information system.
Security	A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach.
Security Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel, and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.
Security Control	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Control Baseline	The set of minimum-security controls defined for a low-impact, moderate-impact, or high-impact information system.
Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment.
Security Objective	Confidentiality, integrity, or availability.

Term	Definition
Security Policy	A set of criteria for the provision of security services.
Security Posture	The security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.
Security Requirements	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Subject	Generally, an individual, process, or device causing information to flow among objects or change to the system state.
Subsystem	A major subdivision or operating unit of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
Supply Chain	A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.
Supply Chain Risk	Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Supply Chain Risk Management	The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains.
System Development Life Cycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation, and maintenance, and ultimately its disposal that instigates another system initiation.
System Security and Privacy Plan	Formal document that acts as both the security plan and privacy plan. Provides an overview of the security and privacy requirements for an information system and describes the security and privacy controls in place or planned for meeting those requirements.
System-Specific Control	A control for an information system that has not been designated as a common control or the portion of a hybrid control that is to be implemented within an information system.
Tailored Control Baseline	A set of controls resulting from the application of tailoring guidance to the security control baseline.
Tailoring	The process by which security and privacy control baselines are modified by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined control

Term	Definition
	parameters; supplementing baselines with additional controls or control enhancements; and providing additional specification information for control implementation.
Technical Controls	The safeguards or countermeasures for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware operating units of the system.
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
User	Individual, or system process acting on behalf of an individual, authorized to access an information system.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Appendix C: Roles and Responsibilities

Designation of Roles

The DOC CIO, operating unit CIO, CISO, operating unit CISO, SAOP, CPO, operating unit CPO, AO, and Risk Executive Function (REF) have inherent United States Government authority and must be government personnel. The operating unit CIO, operating unit CPO, or operating unit CISO may assign appropriately qualified individuals, including contractors (free from conflict of interest) to perform the activities associated with the DOC SPA&A Handbook. An operating unit CIO, operating unit CPO, or operating unit CISO designating a role must retain ultimate responsibility for the results of actions performed by individuals serving in the designated role.

Roles and Responsibilities

The following functions assigned to the Department are designated in the table below. Additional roles and responsibilities are documented in the ECP.

Table C-1: Roles and Responsibilities

Role/Office	Responsibilities
DOC CIO	Per the Clinger-Cohen Act of 1996, the DOC CIO advises and assists the Secretary and Deputy Secretary, and other senior staff. The DOC CIO ensures that the DOC plans, acquires, manages, and uses IT in a manner that enhances mission accomplishment, improves work processes, provides sufficient protection for the privacy of personally identifiable information (PII), and uses IT in a way that promotes citizen-centered electronic government and is consistent with all Federal laws and directives. It is the DOC CIO's responsibility to: ▪ Report to the Secretary of Commerce and OMB on the status of the DOC's Enterprise Cybersecurity Program ▪ Carry out responsibilities under the Federal Information Technology Acquisition Reform Act (FITARA) ▪ Appoint a CISO to carry out the Cybersecurity Program in accordance with FISMA ▪ Ensure that operating unit Officials provide cybersecurity protections commensurate with the potential risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of: o Information collected or maintained by or on behalf of the DOC o Information systems used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency ▪ Enforce DOC's cybersecurity policy ▪ Coordinate the evaluations of new and emerging technologies and maintain a central inventory

Role/Office	Responsibilities
	▪ Ensure cybersecurity management processes are integrated with DOC and/or operating unit strategic and operational planning processes ▪ Approve the use of encryption technologies that are not FIPS validated, or National Security Agency (NSA) approved where products are not available ▪ Develop, implement, and manage an enterprise wide POA&M process to correct cybersecurity weaknesses
DOC CISO	The DOC CISO serves as the principal security leader for the DOC, responsible for the oversight and implementation of the Federal Information Security Modernization Act of 2014 (FISMA). The CISO also serves as the DOC CIO's liaison and implementation manager for all matters relating to security and the DOC Cybersecurity Program. It is the DOC CISO's responsibility to: ▪ Develop standards and guidelines for conducting risk assessments and determining security needs ▪ Implement cost effective DOC policies and procedures for related controls to minimize risk to an acceptable level ▪ Provide leadership to the CISO Council and actively participate in the CIO Council to guide the management and implementation of DOC's Cybersecurity Program ▪ Monitor, evaluate, and ensure security controls and techniques are effectively implemented ▪ Develop and maintain a DOC-wide cybersecurity program ▪ Promote a comprehensive cybersecurity training program for privileged and general users ▪ Develop enterprise cybersecurity policy, standards, and handbooks for implementing FISMA and OMB A-130 security requirements ▪ Assess waiver requests for DOC cybersecurity policy, standard, and handbook conformance on behalf of the DOC CIO ▪ Prepare required FISMA reports on behalf of the DOC CIO ▪ Ensure compliance with monthly reporting on the efficacy of operating unit Cybersecurity programs, including the progress of remedial actions ▪ Identify cybersecurity management and reporting tools ▪ Collaborate, assist, and advise operating unit CISOs regarding cybersecurity program matters
Office of Privacy and Open Government (OPOG)	OPOG is comprised of Privacy Analysts responsible for supporting the duties of DOC's SAOP and protecting the privacy and civil liberties of the American people through review, oversight, and coordination of DOC's privacy operations. OPOG Staff are assigned to operating units to provide advice and guidance to operating units, ensure DOC's privacy compliance, develop, and provide DOC privacy training, assist the SAOP in developing DOC privacy policy, prepare privacy-related reporting to the President and Congress, and review the information handling practices of DOC to ensure

Role/Office	Responsibilities
	such practices are consistent with the protection of privacy and civil liberties. It is the OPOG's responsibility to: ▪ Assist operating units throughout the DOC SPA&A process ▪ Assist in identifying all information system privacy requirements for the operating units during each phase of the SPA&A process ▪ Conduct OPOG evaluations of system authorization documentation on behalf of the SAOP ▪ Conduct oversight reviews of operating unit information systems ▪ Conduct training on the DOC SPA&A process ▪ Approve the categorizations of information systems that process PII
Chief Privacy Officer (CPO)	The DOC CPO is the Department's Senior Agency Official for Privacy (SAOP) and is responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks associated with any agency activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems. Consistent with Executive Order 13719 (E.O. 13719) and OMB M-16-24, the DOC CPO is responsible for developing, implementing, maintaining, and overseeing the Department's privacy program. The DOC CPO serves as the Director of OPOG and is the principal advisor to DOC leadership and operating units on privacy matters affecting the mission and operations. In addition to the responsibilities outlined in DOO 20-31,[14] CPO and Director of Open Government (as amended), the CPO is responsible for: ▪ Coordination between DOC's privacy personnel and the DOC CIO, DOC CISO, operating unit CIOs, and other DOC cybersecurity officers, as appropriate ▪ DOC resource planning and management activities considering privacy ▪ Incorporating federal privacy requirements into DOC's enterprise architecture to mitigate risks and ensure that information systems are trustworthy, protected, and resilient ▪ Reviewing IT capital investment plans and budgetary requests to ensure privacy requirements, controls, and identify associated costs. These reviews include any system that processes, displays, or otherwise utilizes PII. Review and approve the categorization of information systems that processes, displays, or otherwise utilizes PII per NIST FIPS Publication 199 and SP 800-60 ▪ Designating which privacy controls are program management, common, information system-specific, and hybrid privacy controls ▪ Identifying assessment methodologies and metrics to determine privacy controls implementation

[14] DOO 20-31, *Chief Privacy Officer and Director of Open Governments.*

Role/Office	Responsibilities
	▪ Developing and maintaining a privacy continuous monitoring strategy ▪ Reviewing authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure compliance with applicable privacy requirements and manage privacy risks, prior to AOs making risk determination and acceptance decisions
DOC OCRM	▪ Develop and maintain the SPA&A Handbook and appendices, which define the requirements for the security and privacy assessment process ▪ Provide oversight of the SPA&A Handbook applicability and implementation ▪ Review the SPA&A Handbook annually and update as needed
Cyber Liaison (CL)	OCRM CLs are assigned to operating units to assist in the advancement of the DOC Enterprise Cybersecurity Program; clarify DOC policy requirements; and create a more concise understanding and implementation of standards, procedures, guidance, and security best practices prescribed by OCRM, CISO, and CIO. It is the OCRM CL's responsibility to: ▪ Assist operating units with implementing the DOC SPA&A process to comply with FISMA ▪ Oversee and support operating units with integrating the RMF into daily cybersecurity practices and throughout the SDLC ▪ Independently review operating unit information system security authorization documentation, and FISMA system inventory ▪ Monitor operating unit assessment of DOC's Core Controls and completion of DOC's Cybersecurity Awareness Training ▪ Conduct training on the Cyber Security Assessment and Management (CSAM) and DOC SPA&A process ▪ Support operating unit's waiver review and submissions, ISCM inquiries, and internal/external data calls ▪ Support operating units during the annual FISMA and financial statement audits ▪ Serve as the primary liaison for OCRM and operating units ▪ Maintain ongoing communications with operating units ensuring enterprise-wide policies, procedures, and security best practices are implemented

At a minimum, operating units must allocate resources to perform the following functions listed in the table below. Operating units may have additional roles within their organization, which can be documented in operating unit-specific SPA&A documentation.

Table C-2: Additional Roles and Responsibilities

Roles	Responsibilities
Operating Unit CIO	▪ Ensure an effective security program is established for the organization, including establishing SPA&A expectations and requirements ▪ Establish supplemental policies to support operating unit's mission needs ▪ Determine the mission and business functions of the organization based on organizational priorities and appropriate level of funding and resources to support the security program ▪ Ensure that systems are covered by an approved security plan, are authorized to operate, and are monitored throughout the system development life cycle ▪ Help guide and inform AO decisions regarding assessor independence ▪ Appoint AOs for information systems subject to SPA&A requirements
Operating Unit CISO	The operating unit CISO has management, oversight, and compliance responsibilities for securing operating unit information systems, networks, and data per FISMA, DOC policies, procedures, and guidance. It is the operating unit CISO's responsibility to: ▪ Implement DOC policies, standards, and guidelines ▪ Ensure operating unit information systems are completing risk assessments and security control testing in accordance with DOC-defined frequencies ▪ Integrate security in the Capital Planning Investment Control process ▪ Assign operating unit roles and responsibilities ▪ Participate in the DOC CISO Council and collaborate with other operating units to evaluate and select cybersecurity tools ▪ Establish procedures ensuring software installed on operating unit information systems complies with copyright law and incorporates it into the information system's lifecycle management ▪ Manage and remediate operating unit-level Plans of Action and Milestones (POA&Ms) in accordance with the DOC POA&M Handbook
Risk Executive Function (REF)	The REF is responsible for aligning information security processes with strategic, operational, and budgetary planning processes. Executives serving the REF must: ▪ Serve in a leadership role that can support DOC's High Value Asset (HVA) program, and Vulnerability Disclosure Program (VDP) required to oversee and implement DOC policy, procedures, and guidance ▪ Direct cybersecurity activities for the operating unit
Operating Unit Chief Privacy Officer (OUCPO)	In accordance with OMB guidance, at the discretion of the SAOP and consistent with applicable law, other qualified agency personnel may

Roles	Responsibilities
	perform particular privacy functions that are assigned to the SAOP. In addition, agencies shall consider establishing privacy programs and privacy officials at sub-agencies, components, or programs where there is a need for privacy leadership in support of the SAOP. In all cases, however, the SAOP shall retain responsibility and accountability for the agency's privacy program, including privacy functions performed by officials at sub-agencies, components, or programs. The DOC CPO, the Department's designated SAOP, has delegated certain responsibilities associated with implementing the Risk Management Framework to operating unit Chief Privacy Officers. The operating unit CPO is an operating unit official responsible for ensuring the operating unit's compliance with privacy requirements and managing privacy risks. It is the operating unit CPO's responsibility to: ▪ Conduct privacy risk assessments and identify applicable privacy requirements associated with the handling of PII ▪ Select privacy controls for information systems that process PII ▪ Implement selected privacy controls for information system that process PII ▪ Review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII and brief the DOC CPO prior to system authorization
Authorizing Official (AO)	The AO is a senior management official or executive with the authority to assume responsibility for operating an information system at an acceptable level of risk. The AO must have the authority to oversee the budget and business operations of the system within the operating unit. It is the AO's responsibility to: ▪ Review and approve information system requirements, System Security and Privacy Plans (SSPP), and Memoranda of Understanding (MOU) / Agreement (MOA) ▪ Be accountable for the risks associated with operating an information system through a formal authorization decision ▪ Issue an ATO with POA&Ms and limitations for information systems under specific terms and conditions ▪ Deny ATOs or halt operational information systems in the presence of unacceptable cybersecurity risks ▪ Review and approve system-level risk acceptance decision ▪ Review security controls for scoping and tailoring Consistent with OMB Circular A-130 and NIST SP 800-37, the DOC CPO is responsible for reviewing the authorization package for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII, to ensure that privacy risks are managed prior to system authorization. In situations where the AO and CPO cannot reach a final resolution regarding the appropriate protection for the agency information and information system, the head of the agency must review the associated

Roles	Responsibilities
	risks and requirements and make a final determination regarding the issuance of the ATO.
Authorizing Official Designated Representative	The AO's designated representative is an operating unit official acting on behalf of the AO to coordinate and carry out the activities required during the authorization of an information system. However, an AO's designated representative only serves in an advisory role and cannot grant an ATO. The AO's designated representative is responsible for: ▪ Interacting with the System Owner (SO), Information System Security Officer (ISSO), Information System Privacy Officer (ISPO), PCA, SCA, User Representative(s), and other interested parties during the security authorization process ▪ Working with the SO, ISPO, and ISSO to prepare the final authorization package and obtain the AO's signature on the authorization decision document
Common Control Provider (CCP)	The CCP is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (i.e., controls inherited by information systems). It is the CCP's responsibility to: ▪ Document the organization-identified common controls in a SSPP and make it accessible to the common control inheritor ▪ Ensure implementation and assessment of common controls and that there is an appropriate level of independence, as defined by the DOC ▪ Document assessment findings in a Privacy Assessment Report (PAR) or Security and Privacy Assessment Report (SPAR) and make it accessible to the common control inheritor ▪ Develop POA&Ms for all control deficiencies and make it accessible to the common control inheritor Upon the CCP's approval of inherited controls, SOs can access the SSPP, PAR, SPAR, and POA&Ms as necessary.
System Owner (SO)	The SO provides overall procurement, development, testing, integration, modification, or operation and maintenance of the information system. It is the SO's responsibility to: ▪ Assist with developing and maintaining the SSPP, and related system security and privacy documentation to ensure compliance with DOC's security requirements ▪ Conduct oversight of information system POA&Ms ▪ Determine access to the information system, including privilege types or access rights. ▪ Ensure system users and support personnel receive security and privacy training

Roles	Responsibilities
	▪ Inform officials of the need and ensure resource availability to conduct a control assessment and authorization of the information system ▪ Provide the PCA and SCA with required system-related documentation ▪ Implement pertinent controls to reduce or eliminate vulnerabilities ▪ Work with the ISPS and ISSO to assemble the authorization package for AO adjudication ▪ Notify the AO, ISPO, and ISSO of changes that might affect information system accreditation ▪ Review and update all information and content residing in CSAM at least monthly to reflect the current FISMA System security and privacy posture ▪ Support the ISSO and ISPO with creating and maintaining the information system's Contingency Plan ▪ Ensure the completion of all system retirement and disposition activities
Information Owner/Steward	The Information Owner is the operating unit official with statutory or operational authority for information associated with an information system. They are responsible for establishing the controls for the information's generation, collection, processing, dissemination, and disposal.
Information System Security Officer (ISSO)	The ISSO and ISPO supports the AO or other senior management official to ensure operational security and privacy posture maintenance for an information system or program. The ISSO and ISPO serves as the principal advisor to the AO and SO on all matters involving security and privacy of the information system. It is the ISSO's and ISPO's responsibility to: ▪ Assist in the identification, implementation, and assessment of security, privacy, and common controls ▪ Work with system stakeholders to develop the SSPP, SPAR, PAR, Information System Contingency Plan (ISCP), Incident Response Plan (IRP), Breach Response Plan (BRP), Configuration Management Plan (CMP), MOU/A, Interconnection Security Agreements (ISA), POA&Ms, and related information system documentation ▪ Ensure common controls are available for inheritance by other information systems ▪ Ensure systems are operating, maintaining, and disposing of information and data in accordance with DOC policies and procedures ▪ Report and support the SO with all security and privacy related incidents ▪ Monitor system recovery processes and ensure proper restoration of information system security features

Roles	Responsibilities
	▪ Perform self-security control assessments and ISCM activities in accordance with DOC ISCM Handbook frequencies ▪ Serve as a member of Configuration Control Board (CCB) to ensure configuration management for Cybersecurity-relevant software, hardware, and firmware is maintained and documented ▪ Address information system security and privacy requirements during all phases of an information system lifecycle ▪ Review system audit logs, maintain evidence of review, and report completion of audit log review to the SO ▪ Review and analyze automated scan results and work with stakeholders to document remediation activates. ▪ Monitor the security and privacy posture of the information system and report any anomalies to the AO and SO
Information System Privacy Officer (ISPO)	The ISPO is an additional role to be designated at the discretion of the operating unit CPO. The ISPO is responsible for supporting the AO, SO, and ISSO throughout the RMF to ensure PII or BII is protected appropriately.
Information Security Architect	The Information Security Architect is an individual, group, or organization responsible for: ▪ Ensuring the information security requirements protect the operating units core missions and that business processes are adequately addressed in all aspects of enterprise architecture ▪ Serving as the liaison between the Enterprise Architect (EA) and the Information System Security Engineer (ISSE) ▪ Coordinating with the SO and ISSO on the designation of controls as system-specific, hybrid, or common ▪ Coordinating with ISSOs to advise AOs, SOs, CISOs, and CIOs, and key stakeholders on a range of security-related issues like information system boundaries, system deficiencies, POA&Ms, risk mitigation, security alerts, and potential adverse effects of vulnerabilities
Information System Security Engineer (ISSE)	The ISSE is part of the system engineering process used to address users IT protection needs. It is the ISSE's responsibility to: ▪ Ensure the defined cybersecurity solutions are effective and meet all requirements identified by the AO ▪ Ensure development and design of new information systems include appropriate cybersecurity features and safeguards per DOC policies and procedures ▪ Ensure that information system enhancements provide equivalent or enhanced effectiveness of the existing cybersecurity features and remain consistent with DOC and operating unit policies ▪ Assist the development and implementation of the information system security design

Roles	Responsibilities
	▪ Assist the SO and ISSO prepare security authorization documentation ▪ Conduct cybersecurity reviews for information system integration and complete cybersecurity configuration for control assessment testing ▪ Assist the development and review of the security and privacy assessment plan ▪ Coordinate cybersecurity related issues with the ISSO and notify system stakeholders of any changes that may affect the information system security design
Security Control Assessor (SCA)	The SCA is an individual, group, or organization that conducts independent security control assessments for information systems. The SCA is not responsible for developing the SSPP or related information system security documentation such as the ISCP, IRP, CMP, MOU/A, ISA, or information system Standard Operating Procedures (SOP). It is the SCA's responsibility to: ▪ Assess the SSPP to ensure it provides sufficient security control implementation status to meet DOC security requirements ▪ Develop the security and privacy assessment plan, conduct security control assessments, perform, and analyze vulnerability scans, document the SPAR, and provide an authorization recommendation to the AO ▪ Assess changes to the information system, its environment, and operational needs that may affect its authorization status ▪ Recommend POA&Ms to reduce risk to an acceptable level
Privacy Control Assessor (PCA)	The PCA may be designated by the operating unit CPO, when appropriate, to assess privacy controls for information systems. The responsibilities of the PCA will be defined in the security and privacy assessment plans, in support of the AO and SCA.

Appendix D: Information System Registration Process

Introduction

The DOC requires an information system that collects, processes, transmits, stores, and disseminates DOC information to have an inventory in the CSAM application, the system of record for DOC's information system inventory. The SO or designee must follow the operating unit CSAM procedures for CSAM profile information system registration.

System Profile

The SO and ISSO must follow the operating unit CSAM procedures to create an information system profile based on the following information:

Table D-1: System Profile

#	Name	Provide	Requirements:
1	**System Type Determination**		
1A	Inventory Designation	System, Subsystem, Site, or Program	Account for mission, business, and technical requirements; privacy/security considerations; and Personal Identifiable Information (PII)/ Business Identifiable Information (BII) use Site: Physical or data center location of information system operating units; most often utilized as common control providers Program: Entities producing policy documentation or provide high-level shared services (i.e., incident response). Programs are most often utilized as common control providers Reference: NIST Special Publication (SP) 800-37 Rev. 2
2	**System Name and Acronym**		
2A	System Name and Acronym	Establish the information name and acronym	Must clearly distinguish and accurately represent the information system but recommend not using the vendor's name which can associate the information system to a particular technology. Once the information system name is entered into CSAM, the field is locked and can only be changed by a CSAM administrator upon approval from the assigned AO
3	**Operating Unit/Sub-Operating Unit**		
3A	Operating Unit	Assign responsible operating unit	The management office and ownership of the information system

#	Name	Provide	Requirements:
4	**Mission**		
4A	Mission	A description of the mission the system supports	High-level description of the mission the information system supports, primary function or service, and information system capabilities
5	**Operational Status Determination –** *Choose one status*		
5A	Operational Status	LIST STATUS AS:	WHEN SYSTEM IS IN:
		Initiation	Risk Management Framework (RMF) Step 1, RMF Step 2, RMF Step 3
		Development	RMF Step 4, RMF Step 5
		Implementation	RMF Step 6: Authorize – Does NOT have an ATO
		Operational	RMF Step 6: Authorize – Has ATO, RMF Step 7
		Retired	RMF Step 7 – Completed Disposition
		Modification	Use for non-operational system only, while system is in limited use for modernization, migration, or preparing for retirement.
6	**Financial Status Determination –** *Choose ONE financial status*		
6A	Financial Status System Designation	THE STATUS IS:	WHEN THE SYSTEM:
		Financial	Is directly used for managing and reporting the receipt, disbursement, or recognition of financial obligations due to/incurred by the organization – AND does not provide additional non-financial functions OR Is directly used to support financial planning, budgeting, and official reporting of the financial management information – AND does not provide additional non-financial functions
		Financial Mixed	Directly supports a financial information system, including storing or transmitting financial information OR Is a "Financial" information system that additionally provides non-financial functions

#	Name	Provide	Requirements:
		Non-financial	Does not support, process, store, or transmit financial information
7	**Contractor System Determination –** *Only mark if applicable*		
7A	Contractor System	Contractor System	The information system is operated or hosted by a contractor on behalf of the DOC
8	**Preliminary PII/BII Holding Determination –** *Only mark if applicable*		
8A	Preliminary PII/BII Holding	System contains PII/BII	If the information system creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of PII/BII
9	**FISMA Reportable Determination –** *Choose ONE status*		
9A	Federal Information Security Modernization Act (FISMA) Reportable	FISMA Reportable	As defined by OMB M-24-04, as amended, or the equivalent, for FISMA reporting purposes[15]
		Not FISMA Reportable	The Operational Status is Initiation, Development, Implementation, Modification, or Retired OR The system is a sub-component of another system that is already being reported
10	**Critical Infrastructure Determination**		
10A	Critical Infrastructure	Select "Critical Infrastructure"	Operating unit AO and SO have jointly determined the information system or asset to be so vital to the United States that its incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters. If there is no AO, the Program Sponsor must be involved. *Reference: PPD-21 section 1016€*
11	**Mission Criticality Determination**		
11A	Mission Critical/ Mission Essential	Select "Mission Critical"	Mission Essential Systems (MES) are those information systems that support or enable DOC-identified Mission Essential Functions (MEF) or Essential Supporting Activities (ESA). DOC's MEFs are defined by Office of Security (OSY). Operating unit AO and SO

[15] Systems with an Operational Status set to 'Operational' and a FISMA Reportable status set to 'Yes,' must comply with all FISMA reporting requirements and guidance issued by OMB.

#	Name	Provide	Requirements:
			have jointly determined that the information system's continued operation is so vital that the incapacity or destruction of the information system would have a debilitating impact on DOC mission. **Note: Information Systems can be Critical Infrastructure and Mission Critical.**
12	**High Value Asset Determination**		
12A	High-Value Asset (HVA)	Select "High-Value Asset"	▪ HVA are DOC, Facility, Program, or NSS Information Systems ▪ Complete the HVA ID Tool and enter resulting determination. Until the entire HVA identification process is complete and hasbeen submitted to CISA, HVA flag should be set to NO ▪ Only the DOC CIO can add or remove HVA inventory ▪ Adjustment/edits to HVA inventory if found incorrectly reported can be made by DOC HVA Program PMO ▪ Refer to the HVA Handbook for additional HVA requirements

Discovered Non-Inventory Information Systems or Applications

In the event an unauthorized operational information system is discovered, the SO and ISSO must conduct the following actions:

Table D-2: Discovered Non-Inventory Information Systems or Applications

Step	Action	Description
1	Notify the AO	If an information system is discovered to be operational without an ATO, the AO must be notified immediately
2	Identify a line of authority	Operating unit will determine a responsible line of authority. The Unified Payment Interface (UPI) number used to obtain funding will usually suffice. If no one accepts system responsibility, deactivate and disconnect the system or application
3	Remediation efforts	OCRM Cyber Liaison (CL) will advise the SO or designated operating unit representative on remediating issues effectively and efficiently. Generally, the result is a modification to an existing System Security and Privacy Plan (SSPP) or the initialization of a new SSPP. Both result in information system authorization activities, though the details of the situation determine the level of effort required
4	Conduct a Security Impact Analysis	The SO will perform an assessment to collect sufficient information to: ▪ Characterize the newly discovered information system ▪ Identify an ISSO ▪ Mission need, mission area, and line of business ▪ The data types processed and associated level of concern ▪ Information system scope, authorization boundary, and interconnection
5	Follow the SPA&A Handbook RMF Steps	The SPA&A Handbook is a guide for discovered or legacy information systems or subsystems. Use the characterization and risk assessment results to determine whether it will be handled as part of an existing information system or a new information system inventory
6	Establish a plan for system authorization	Situationally, the AO may determine that: ▪ A complete information system authorization is appropriate ▪ A well-performed and documented risk assessment may support an attenuated information system authorization task focused on specifically impacted controls. An attenuated authorization task may recommend an addendum memorandum to the existing ATO

Appendix E: Security and Privacy Control Tailoring Guide

Introduction

The tailored security and privacy control baseline for an information system must be tailored to provide the appropriate level of protection for the information owner. The tailoring process applies scoping guidance, in accordance with the process defined in this document, to customize the set of controls deemed appropriate for the information system. This process includes removing controls that are not deemed applicable or essential for the information owner as well as potentially including supplemental controls as may be appropriate following the minimum-security requirements established in the FIPS 200.

Security Scoping Considerations

Apply scoping considerations to the initial baseline security controls to obtain a preliminary set of applicable controls for the tailored baseline. Considerations include security objectives, information owner component allocation, technology, physical infrastructure, policy/regulatory drivers, operational and environmental context, scalability, and public access. Scoping guidance provides the operating unit with specific terms and conditions on the applicability and implementation of individual security controls in the baselines.

Potential Security Scoping Considerations

There are several scoping considerations described below that can potentially affect how the baseline security controls are applied and implemented by organizations.

Table E-1: Potential Security Scoping Considerations

Consideration	Scoping Guidance
Security Objective-Related	Security controls that support only one or two of the confidentiality, integrity, or availability security objectives may downgrade to the corresponding control in a lower baseline (or modified or eliminated if not defined in a lower baseline).
System Component Allocation-Related	Security controls apply only to the operating units of the information system that provide or support the security capability addressed by the control and are sources of potential risk mitigated by the control.
Technology-Related	Security controls that refer to specific technologies are applicable only if those technologies are employed or require employment within the information system.
Physical Infrastructure-Related	Security controls that refer to organizational facilities apply only to those sections of the facilities that directly protect, support, or relate to the information system.
Policy / Regulatory-Related	Security controls addressing matters governed by federal laws, Executive Orders, directives, policies, standards, or regulations are only required if the controls' employment is consistent with the information types and information owners covered by the governance.

Consideration	Scoping Guidance
Operational / Environmental-Related	Security controls based on specific assumptions about the operational environment only apply if the assumed environment employs the information system.
Scalability-Related	Security controls are scalable concerning the extent and rigor of the implementation.
Public Access-Related	When public access to organizational information systems is allowed, security controls are applied with discretion since some from the specified control baselines may not apply to public access.

Scoping Out Security Controls

When operating units scope a control out of a baseline, the operating unit must include a specific, clear justification for its exclusion. The detailed explanation must be entered at the assessment screen in the CSAM application and approved by the AO and SO as part of the review and sign-off process for the SSPP. Tailoring of a control baseline without a meaningful justification and documented authorization from the appropriate responsible party is not authorized.

Operating Unit Defined Parameters

Once the baseline controls have been appropriately scoped and tailored, the operating unit should define any open operating unit-defined parameters in the applicable security controls. Some controls have parameters prescribed at the Department level and must remain unchanged unless the operating unit wishes to implement more stringent requirements. Other controls have operating unit-defined parameters, requiring operating units to determine the parameters they assess against. Security controls containing operating unit-defined parameters give operating units the flexibility to define certain portions of the controls to support specific operating unit requirements or objectives. Operating units must send an email request to the OCRM Cyber Liaison containing the operating unit-defined parameters that require modification. The review process by the OCRM Team ensures operating unit-defined parameters meet or exceed DOC Requirements.

Compensating Security Controls

Operating units may find it necessary to employ compensating security controls when an operating unit is unable to implement a security control in the baseline. The inability may be due to the nature of an information system or its environment of operation. It could also be necessary because the control in the baseline is a cost-ineffective means of obtaining necessary safeguards in place of a recommended baseline security control. Controls must provide an equivalent or comparable level of protection for an information system and the information processed, stored, or transmitted by that information owner. More than one compensating control may be required to provide the equivalent or comparable protection for particular security controls. A compensating control may be employed only under the following conditions:

- The operating unit selects the compensating control from NIST SP 800-53 Rev. 5, or if an appropriate compensating control is not available, the organization adopts a suitable compensating control from another source
- The operating unit provides a supporting rationale for how the compensating control delivers an equivalent security capability for the information system and why the related baseline security control could not be employed
- The operating unit assesses and formally accepts the risk associated with employing the compensating control in the information system

Security Controls Overlays

Operating units may supplement the tailored baseline with additional security or privacy controls or control enhancements to address specific threats to and vulnerabilities in the information system and to satisfy the requirements of applicable Federal laws, Executive Orders, directives, policies, standards, or regulations. In many cases, operating units need additional security or privacy controls or control enhancements to address specific threats to and vulnerabilities in an information system. Based on the results of a Security Risk Assessment, Security Control Assessment, Supply Chain Risk Assessment, Privacy Risk Assessment or other security and privacy requirement identification activities, operating units may supplement the tailored baseline with additional security and privacy controls commensurate with the risk to the information system. Furthermore, operating units may employ gap analysis to identify supplemental controls that address critical threats to the information system. If the operating unit's current security capability or level of preparedness is insufficient, the gap analysis determines the required capability and level of preparedness. For additional information, refer to Section 4.4 Select Security and Privacy Controls of the SPA&A Handbook.

Privacy Controls

Privacy controls are administrative, technical, or physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and to manage privacy risks. Privacy risks can include risks beyond those typically included under the confidentiality prong of the information security triad. Agencies shall use privacy controls to manage all privacy risks, regardless of whether those risks would be considered information security risks. To help operating units satisfy privacy requirements and manage privacy risks, NIST developed a set of privacy controls, based on the Fair Information Practice Principles, in NIST SP 800-53 Rev. 5. The DOC used the NIST privacy controls to develop its tailored privacy control selection process for information systems. If the OPOG determines that an information owner does not create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII, mark the privacy controls as N/A in CSAM.

The DOC CPO is responsible for designating which controls DOC treats as program management, common, information system-specific, and hybrid controls. Privacy program management controls

are controls that are generally implemented at the agency level and essential for managing the DOC's privacy program.

When the operating unit assigns privacy controls to an information system as information system-specific, hybrid, or common controls, they assign responsibility and accountability to specific operating unit programs or officials for the overall development, implementation, assessment, authorization, and monitoring of those controls. In all cases, the CPO must maintain oversight and coordinate privacy control management.

Appendix F: Security and Privacy Control Assessment Process

Introduction

The security and privacy control assessment consists of testing the implemented functionality of the information systems to ensure the information system is deployed in a secure manner consistent with the information system's categorization and applicable requirements regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposition of PII/ BII and other regulated data types. Before any testing, the operating unit must ensure the SCA and PCA have the required degree of independence.

Roles and Responsibilities

Independent Control Assessor

An Independent Control Assessor is an individual capable of conducting an impartial assessment of security or privacy controls within an information system. Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, or management of the information system or the determination of security or privacy control effectiveness. Independent security or privacy control assessment services can be obtained from other elements within the operating unit or contracted to a public/private sector entity outside of the organization. Contracted assessment services are independent if the SO is not directly involved in the contracting process or cannot unduly influence the independence of the SCA or PCA.

An Independent SCA may also be selected as the Independent PCA if the individual is capable of conducting an impartial assessment of both the privacy and security controls. The AO must determine the independence level required for SCA and PCA based on the assessment requirement, results of the information systems categorization process, and the ultimate risk to organizational operations, assets, individuals, other organizations, and the Nation. The independence level of the SCA and PCA independence must be sufficient to provide confidence that the assessment results produced are sound and can be used to make a Risk Based decision on whether to place the information system into operation.

If the SCA is not required to be independent, the operating unit must employ an AO to review and approve the assessment results. Regardless of the independence of the PCA, the operating unit must employ a Privacy Risk Authorizing Official to review and approve the assessment results prepared by the PCA. Unless designated otherwise by the CPO, the operating unit CPO shall serve as operating unit's Privacy Risk Authorizing Official.

For the annual control assessments conducted for OMB Circular A-123, the operating unit-designated reviewer must document conclusions in the CSAM application relative to their review. For all other control assessments for which the assessor is not required to be independent, the AO must prepare an Authorization Memo indicating his or her recommendations on the authorization of the information systems.

Security Control Assessor

The SCA must assess the applicable security controls and information systems-specific portions of the hybrid security controls using assessment methods specified in CSAM, as described below. The SCA may also serve as the Privacy Control Assessor, so long as the individual can conduct an impartial assessment of both the privacy and security controls employed within a system.

Privacy Control Assessor

The PCA must assess the applicable information systems-specific privacy controls, and the information systems-specific portions of the hybrid privacy controls, using assessment methods specified in CSAM, as detailed below. The CPO is responsible for identifying assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and ensuring compliance with privacy requirements and managing privacy risks. The CPO is also responsible for conducting and documenting the results of privacy control assessments to verify the continued effectiveness of all privacy controls implemented across all DOC risk management tiers, ensuring continued compliance with privacy requirements and privacy risk management.

All PCA must be approved by the operating unit CPO, or equivalent delegate, before starting the privacy control assessment process. The PCA may also serve as the SCA, so long as the individual can conduct an impartial assessment of both the privacy and security controls employed within an information system.

Control Assessment Methods and Processes

Assessment methods define the nature of the assessor's actions and include examination, interviewing, and testing.

1. The examine method is the process of reviewing, inspecting, observing, studying, or analyzing. The purpose of this method is to facilitate assessor understanding, achieve clarification, and obtain evidence. It is often used with policies, procedures, or other documented results.
2. The interview method is the process of holding discussions to facilitate assessor understanding and achieve clarification. In most cases, interviews alone are not sufficient to consider testing complete.
3. The test method is the process of exercising activities or mechanisms under specified conditions to compare actual with expected behavior. The results in all three assessment methods help make specific determinations needed in the Determine If statements and thereby achieving the objectives for the assessment procedure.

The content entered into the CSAM application during testing must indicate the assessor’s finding (conclusion) relative to the expected result from the Determine If statement. This content must be fully responsive to all requirements in the Determine If statement as they relate to all operating units within the information system boundary.

For any hybrid applicability scenario, the assessor must identify the aspects that are not applicable and include the rationale for the non-applicability. For each finding of Other than Satisfied, the assessor describes in the CSAM Finding field the aspects of the control that were deemed not satisfied or were not able to be assessed and describes how the control differs from the expected result. The assessor must indicate in the Methods and Objects field the method(s) used to assess the control and the object(s) relied on to arrive at the assessment conclusion documented in the Finding field. The methods and objects must be described in sufficient detail to allow an individual with a similar background with no knowledge of the information systems to repeat the assessment and arrive at the same conclusion.

Manual assessments for controls shall include:

- Reviews based on the depth and breadth determination of existing information systems technical documentation
- Interviews with knowledgeable personnel
- Physical observation and inspection of information systems hardware, software, and procedures where possible
- Manual and script-based testing

Additionally, the SCA must use automated tools for vulnerability scanning and security configuration compliance. The purpose is to determine the network topology, configuration, and information systems application vulnerabilities via scans. Manual reviews of the scan results are conducted that validate the findings of the automated scans. The vulnerability scans shall:

- Verify the proper implementation of security policies
- Verify that secure baseline configurations have not changed. If changes are present, documentation must be present, justified, and subsequent authorization testing or annual assessments conducted to ensure that changes do not affect the security posture of the information systems
- Determine the topology details, allowing the operating unit to evaluate the topology for potential security vulnerabilities
- Examine hosts for the presence of problems and configurations with the potential for exploitation. This action allows the team to identify potential configuration issues and related vulnerabilities to address
- Perform network-based scans according to the operating system(s) or function(s)
- Be conducted in a series of data gathering steps consistent with the methods established for the information systems analysis

The operating unit must provide the assessor with all supporting assessment-related materials needed to conduct an effective assessment and examine opportunities for reusing assessment results from previous assessments or other sources. The SCA and the PCA must complete the control assessment following the stated assessment plan. The ISSO must coordinate the availability

of necessary resources to assist the assessment team as needed or requested. The result of a control assessment can only be one of the following:

- **Not Applicable (N/A)** – is a result where the requirement was determined not to be required in RMF Step -2: Security and Privacy Control Selection, via the use of scoping guidance. This result must have a valid justification supplemented.
- **Satisfied** – is acceptable where the SCA and PCA have developed a reasonable judgment that the determination statement of the control has been implemented as designed, operating as intended, and integrated with the management of the information system. A subsequent review of the assessment and artifacts should be able to arrive at the same result objectively. SCAs must indicate variances from the prescribed test steps in the findings, including the use of compensating controls.
- **Other than Satisfied** – is required where the SCA and the PCA cannot develop a reasonable judgment that the determination statement is implemented as designed, operating as intended, and integrated into the management of the information system. Reaching this particular result requires that the SO either develop a POA&M to address the weakness or request a waiver. For more information, please reference RMF Task 5-1: Plans of Action and Milestones.
- **Waiver** – is an indication that the AO has made an informed decision that the policy's implementation cannot achieve the required degree of success. The outcome of the waiver process is a memo. Controls linked to the process of requesting a waiver must assess the control as Other than Satisfied and create a POA&M to document the deficiency to include relevant milestones. For information system-level security controls, upon completion of the waiver request and signed approval by the AO, operating units must upload supporting documentation to CSAM as an artifact for the POA&M. For operating unit-wide security controls, upon completion of the waiver request and signed approval by the AO, operating units must send the waiver request to OCRM for DOC CIO decision. Upon approval and concurrence of the request, operating units must upload supporting documentation to CSAM as an artifact of the POA&M. The SCA must then reassess the control and choose the waiver option in CSAM. For privacy risks, upon completion of the request template and signed approval by the AO, the operating unit must send the waiver request to DOC's OPOG for concurrence. OPOG must concur before the privacy-related waiver memo finalization. Upon approval and concurrence of the request, supporting documentation must be uploaded to CSAM as an artifact, and the POA&M must be closed. The PCA must then reassess the control and choose the waiver option in CSAM.

Security Control Risk Acceptance

A risk acceptance is required for information system-specific security control weaknesses that result in POA&Ms, or information system-level risks identified through Assessment and Authorization, Continuous Monitoring, Vulnerability Management, etc. Risk acceptance may be appropriate for weaknesses that are not able to be immediately resolved and/or where the resulting

weakness is partially mitigated by compensating controls. Risk acceptance may be documented and approved in a risk acceptance memo by the system's AO or by the operating unit CIO.

Additionally, risk acceptance may be needed when a control in a system's selected baseline is not implemented for one of the following reasons[16]:

- The implementation of the control adversely impacts operations and impairs the operating unit's/information system's ability to meet its mission and objectives
- The technology does not currently exist or is not feasible to provide an effective solution to satisfy the control requirements
- The cost of implementing the control outweighs the benefits as a result of a cost-benefit analysis

Operating units may not utilize a risk acceptance for outstanding risks which would result in DOC's non-compliance with a legal requirement or an independent audit finding (i.e., Office of Inspector General (OIG), the Government Accountability Office (GAO), and Cybersecurity and Infrastructure Security Agency (CISA)). Risks requiring acceptance are distinct from controls that were determined not to be required in (RMF Step tailored out of the baseline (RMF Task S-2, Select Security and Privacy Controls. Certain controls can be implemented with mitigating solutions that may not require acceptance of risk when the mitigation reduces the risks to an acceptable level.

Operating units must review risk acceptances annually to determine applicability and address changes to the evolving information system's environment. The expiration date must not extend beyond the expiration date of the information system's ATO. At a minimum, risk acceptance memos require formal documentation of the following information:

- Reference to the policy statement, enhancement, and excerpt of the description
- Compensating security or privacy controls implemented to mitigate the deficiency or vulnerability including the source of the weakness
- Risk level of deficiency or vulnerability from risk assessment
- Potential impact on information and IT system if exploitation of weakness occurs
- Comprehensive rationale and justification for risk acceptance
- Mitigation strategy describing actions or decisions that would change the risks and weaknesses identified, such as technology refresh, analysis of alternatives, modernization initiatives, or resource allocation
- Date of expiration for the request

[16] RMF Task I-2 Update Control Implementation Information

Appendix G: Cloud Service Provider Assessment Guide

Cloud Service Provider Assessment Requirements

A key element to successful adoption of cloud services is to ensure essential security controls are properly implemented and effective security management based on risk management and compliance is applied. This guide addresses the process and procedures associated with completing security assessments, authorization, and continuous monitoring activities for CSPs. It identifies and defines the resources, responsibilities, processes, and artifacts necessary to guide the successful authorization of cloud computing products and services.

By following this process, DOC operating units will be able to increase the agility, efficiency, and effectiveness of DOC security practices in authorizing and utilizing cloud computing products and services that have successfully completed a FedRAMP authorization process,

CSP Security and Privacy Assessment & Authorization

When applied to CSPs, SPA&A processes and procedures must align with existing policy, standards, and guidance to ensure security and privacy controls for DOC information systems deployed in the cloud are selected, implemented, and assessed in accordance with established DOC and FedRAMP requirements. FedRAMP Security Authorization processes[17] require assessment, authorization, and continuous monitoring of cloud systems in accordance with FISMA.

In accordance with OMB M 24-15, the DOC promotes operating units' prioritization of cloud computing products and services that meet FedRAMP security requirements and other risk-based performance measures, as determined by OMB in consultation with the General Services Administration (GSA) and CISA.

The activities described under this section have specific relevance to cloud environments and shall be completed as a part of the DOC's effort to promote effective management and oversight of security and privacy considerations in accordance with applicable DOC and Federal policies, standards, and procedures.

Successful completion of a FedRAMP authorization process does not fully replace existing DOC operating unit assessment and authorization activities and responsibilities outlined in the DOC SPA&A Handbook. Rather, an existing FedRAMP authorization allows DOC operating units to review the assessment artifacts for risk analysis and to save time and resources in obtaining agency ATO for deploying and implementing cloud services.

[17] Current high-level information about the FedRAMP framework can be found on https://www.fedramp.gov/federal-agencies/. In addition, there are two core documents that describe the FedRAMP authorization process from the CSP's and Agency's perspective - the CSP Authorization Playbook and Agency Authorization Playbook.

FedRAMP Scope

The scope of the FedRAMP program includes all cloud[18] computing products and services that create, collect, process, store, or maintain federal information on behalf of a federal agency and are not otherwise specified as being outside the scope of the program.

The following categories of cloud computing products and services are considered outside the scope of FedRAMP and thus do not require a FedRAMP authorization:

- Information systems that are only used for a single agency's operations, hosted on cloud infrastructure or platform, and are not offered as a shared service or do not operate with a shared responsibility model
- Social media and communications platforms used in accordance with agency social media policies. Refer to the Office of Public Affair's (OPA) list of approved social media services and online platforms[11]
- Search engines
- Widely available services that provide commercially available information to agencies, but do not collect Federal information
- Ancillary services whose compromise would pose negligible risk to Federal information or information systems, such as systems that make external measurements or only ingest information from other publicly available services
- Any other categories of products or services identified for exclusion by the FedRAMP Board, with the concurrence of the Federal CIO

Operating units are responsible for assessing the risk of using these products and services even though a FedRAMP authorization is not necessary.

FedRAMP authorization only applies to information systems that process unclassified information. It does not apply to national security systems as defined in 44 U.S.C. 3552.

Types of FedRAMP Authorizations

There are currently two types of FedRAMP authorizations[19]: agency authorizations and program authorizations.

[18] See NIST SP 800-145 for a definition of cloud computing at https://csrc.nist.gov/pubs/sp/800/145/final.

[11] See https://connection.commerce.gov/rules-and-standards/approved-social-media-services-and-online-platforms

[19] FedRAMP is currently developing additional and alternative FedRAMP authorization pathways. For the most up-to-date information, please review available authorization pathways listed under the 'Get Authorized' page on www.fedramp.gov.

FedRAMP Agency Authorization

Agency authorizations can either be conducted by a single agency or jointly by multiple agencies. In both scenarios, a Federal agency's AO attests that the agency or joint group of agencies assessed a CSP's security posture in accordance with FedRAMP guidelines and found it acceptable.

An existing agency authorization may make it easier for the Department's operating units to deploy new applications quickly; however, this does not guarantee that an agency authorization equates to an automatic approval for use by DOC. For example, the DOC may determine additional customer responsible controls are necessary after completing authorization readiness assessment activities.

The FedRAMP agency authorization path involves an agency partnering with a CSP on an initial FedRAMP authorization. When partnering with a CSP through the agency authorization process, an agency works directly with the CSP, performing a quality and risk review of all information included in its authorization package. The CSP works directly with the agency information technology security office and presents all documentation to the agency AO for an authorization.

An agency authorization indicates that the agency has completed a quality and risk review in accordance with FedRAMP guidelines, identified any customer/agency responsible controls needed, and that the CSP has met FedRAMP and agency-specific requirements making it acceptable for use and authorization. The FedRAMP Program Management Office (PMO) reviews FedRAMP agency authorization packages for compliance, issues an Agency Review Report, and if approved, updates the CSP status on the FedRAMP Marketplace to "FedRAMP Authorized."

FedRAMP Program Authorization

A program authorization is signed by the FedRAMP Director and indicates that FedRAMP assessed a cloud service's security posture and found that it met FedRAMP requirements and is acceptable for reuse by agency AOs.

Authorization Readiness Assessment

DOC operating units must complete a quality and risk review of a CSP's authorization package to conclude the CSP's ability to meet and support FedRAMP, Department, and operating unit-specific security requirements. Requirements are determined by the risk level of the underlying contract and business need, and may include:

- US citizen personnel
- Contiguous United States data centers
- Homeland Security Presidential Directive 12 (HSPD-12) support
- Federal Information Processing Standards (FIPS) 140-2 (or higher) validated encryption at rest and in transit (e.g., TLS 1.2 or higher)
- Identification of all third-party vendors in its interconnection table, logical and physical separation for its customers
- Domain Name System Security Extensions (DNSSEC) usage

- CSPs support TIC policy enforcement points and other protections described in the TIC 3.0 Reference Architecture and TIC 3.0 Security Capabilities Catalog
- Ability to import audit logs into DOC enterprise Security Information and Event Management (SIEM) tools
- Ability to block out all IP addresses except for DOC approved IP addresses
- Ability to comply with the DOC ECP, SPCM, DOC-defined cybersecurity standards (e.g., defined log and data retention schedules, session lock configuration, incident reporting process, etc.), Secure Software Development Attestation memo[20], as well as others

The quality and risk review process requires agencies to evaluate safe, secure, cloud computing options before making any new investments. It allows the DOC operating unit to provide questions and concerns to the CSP and to better understand the risk posture of the CSP-implemented security controls. This process may include in-person working sessions to address specific areas of the CSO and conference calls. Timely DOC operating unit feedback is critical to the overall project schedule. A strategic approach to remediating DOC operating unit questions and concerns should be applied and may include tracking and updating questions and concerns in a workbook, and the CSP and third-party assessment organization (3PAO) completing iterative remediation activities.

When seeking use of a CSO that is already FedRAMP authorized, the DOC operating unit must review the CSP's most recent SPAR and at least the last 90 days of continuous monitoring deliverables to have a full understanding of the CSP's current risk posture. The goal is to obtain early feedback on whether a CSO is likely to be granted a DOC-level authorization.

In accordance with the presumption of adequacy[21] of FedRAMP authorizations, operating units should assume that 3PAOs or partners of FedRAMP authorizations are acceptable for meeting CSO responsible controls as defined in the Customer Responsibility Matrix (CRM). Though, due diligence is necessary to evaluate and confirm that a CSO's security posture and service level agreement meet DOC policy, standards, contract terms, and business need before DOC acquiring the service.

In the course of reviewing a FedRAMP-authorized CSO's authorization package, if an operating unit AO identifies a "demonstrable need" for security requirements beyond those reflected in the FedRAMP authorization package, or if the information in the existing package is found to be wholly or substantially deficient for the purposes of performing an authorization, the operating unit may perform additional work and conduct further assessments to confirm the adequacy of the CSO.

If a new authorization is issued following additional work, the operating unit that performed the additional work must document the reasons for finding the previous FedRAMP package deficient

[20] See OMB M-23-16, Update to Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*.

[21] OMB M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*

and share this information with the DOC OCRM and FedRAMP PMO. Alternatively, the program office may review comparable CSOs to identify a solution that meets all requirements and adequately demonstrates a satisfactory authorization package.

When considering migrating a DOC information system to a FedRAMP authorized CSO, the AO should also consider the following about the DOC information system:

- Is the DOC information system's ATO active?
- Are the risk impact levels equal or greater than the current environment?
- Has a security impact analysis been completed to document proposed changes and their impacts to the current and future environments?
- Have appropriate capital planning and investment control steps been followed?
- Are vulnerability scans current?
- Are there any critical or high vulnerabilities? If so, are they on schedule to be remediated?
- Are there any delayed POA&Ms? If so, why are they delayed and what is the remediation status?

Cloud System Risk Management Framework

The required SPA&A activities for cloud services are equivalent to those identified in the DOC SPA&A Handbook with the exception of a few distinct activities that are unique for cloud environments. This section will list the distinct cloud assessment and authorization activities. These activities are subordinate to the existing DOC SPA&A Handbook and do not replace the DOC SPA&A required process and procedures in support of granting an authorization of an information system.

The issuance of a separate Authorization to Test (ATT) or ATO is required for DOC information systems (e.g., applications) that are migrated or developed on top of an IaaS or PaaS cloud service model (optional for SaaS). The scope of the DOC's implementation and assessment of security control requirements assigned via the CSP Control Implementation Summary (CIS)/CRM workbook only addresses the operating unit's use and operation of the CSO and not the DOC information system hosted in the cloud. Operating units are responsible for providing security measures to the controls listed in the CRM where the CSP offers partial or no controls.

Operating units looking to migrate to cloud environments must use the Cloud Security Technical Reference Architecture[22] developed by CISA and FedRAMP. The ATT or ATO for DOC information systems hosted in the cloud is not reviewed by FedRAMP and is not in-scope when granting an authorization of use for a CSO.

A FedRAMP authorization only assesses vendor side security controls. For any operating unit's authorization of a CSP, that operating unit must also determine all applicable operating unit-

[22] https://www.cisa.gov/cloud-security-technical-reference-architecture

specific FISMA controls and perform a full SPA&A on those controls as part of the authorization package.

CIS/CRM Workbook

During RMF Step 2-Select Security and Privacy Controls, operating units must use the CIS/CRM workbook to tailor security controls for a cloud system in CSAM using the NIST SP 800-53 Rev. 5 security controls to establish the security baseline. The FedRAMP security control baseline can contain controls above the NIST provisional control baseline which address the unique elements of cloud computing. An operating unit must review and consider the risk associated with the CSO and use to determine applicability to its operation.

The CIS/CRM workbook contains a matrix outlining which controls are CSP-provided, agency/customer-provided, and hybrid according to the following security and privacy control origination definitions.

Table G-1: Security and Privacy Control Definitions

Control Origination	Definition	Example
Service Provider Corporate	A control that originates from the CSP corporate network.	Domain Name System (DNS) from the corporate network provides address resolution services for the information system and the service offering.
Service Provider System Specific	A control specific to a particular system at the CSP and the control is not part of the service provider corporate controls.	A unique host-based intrusion detection information system (HIDs) is available on the service offering platform but is not available on the corporate network.
Service Provider Hybrid	A control that makes use of both corporate controls and additional controls specific to a particular information system at the CSP.	Scans of the corporate network infrastructure; scans of databases and web-based application are information system specific.
Configured by Customer	A control where the customer needs to apply a configuration to meet the control requirement.	User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http or https, etc.), entering an IP range specific to their organization are configurable by the customer.
Provided by Customer	A control where the customer needs to provide additional hardware or software to meet the control requirement.	The customer provides a solution to implement two-factor authentication.
Shared	A control that is managed and implemented partially by the CSP and partially by the customer.	Security awareness training must be conducted by both the CSP and the customer.

Control Origination	Definition	Example
Inherited from pre-existing Authorization	A control that is inherited from another CSP information system that has already received an Authorization.	A Platform as a Service (PaaS) or Software as a Service (SaaS) provider inherits Physical and Environmental Protection Policy and Procedures (PE) controls from an Infrastructure as a Service (IaaS) provider.

Controls that fall under Service Provider Corporate, Service Provider System Specific, Service Provider Hybrid, and Inherited from pre-existing Authorization designations are controls that should be selected and tailored externally applicable. Controls that fall under Configured by Customer and Provided by Customer are controls that should be selected and tailored as applicable. Controls that are shared should be selected and tailored as externally hybrid. Externally hybrid tailoring requires the ISSO or SCA to mark the appropriate control or determine if statement as "hybrid" when prompted.

For IaaS and PaaS service models that have a different FIPS 199 impact level than the DOC operating unit information systems that it will host, the DOC operating unit must conduct a security impact analysis to consider the operational and management responsibilities associated with an IaaS and PaaS when tailoring the DOC designated controls.

The DOC operating unit should do an analysis of the CSO control baseline to understand what controls a CSP is required to implement and to address any delta of controls outside of the adopted FedRAMP baseline.

If the DOC operating unit wishes to take full or shared responsibility of a CSP designated control, then the DOC operating unit should inquire with the CSP on its justification of the control responsibility designation. The DOC operating unit can re-designate a CSP-responsible control as its own responsibility as well as add additional controls to its information system control boundary. In the event that this occurs, the DOC operating unit must then implement and assess those additional controls. The final control baseline should be agreed upon between the DOC and the CSP.

Implementing and Assessing Security and Privacy Controls

During RMF Steps 3 and 4 – Implementing and Assessing Security and Privacy Controls, CSPs implement a large portion of security and privacy controls depending on the cloud service model (e.g., SaaS, PaaS, and IaaS). Once the DOC operating unit selects the security and privacy controls in CSAM, the DOC operating unit must implement those controls and document how they use or plan to use the CSO in support of their business and mission needs in the DOC operating unit information system-level security and privacy plan in CSAM. This process will require the DOC operating unit to develop information system-level documentation and artifacts in support of assessing controls and requesting an authorization.

During the assessment of Customer System Specific and Customer Responsibility designated controls, the utilization of FedRAMP documentation as artifacts to verify operating unit implementation of a CSO is not acceptable, and storage of FedRAMP documentation in CSAM should not occur.

Plan of Action and Milestones Management

Per the DOC POA&M Handbook, when drafting a POA&M to brief the AO, the DOC operating unit should summarize open CSP POA&Ms along with a detailed listing of DOC operating unit information system-level POA&Ms during reporting. This activity will give the AO insight into inherited risk and will allow the AO to monitor the progress of the DOC operating unit and the CSP correcting weaknesses or deficiencies noted during the security and privacy control assessment activities.

Authorization Process

During RMF Step 5 – Authorize Information System, the AO must be briefed on the current security and privacy posture of the CSO (e.g., 3PAO security assessment results, POA&M report, vulnerability assessment scan report, non-remediated information system and documentation issues discovered by DOC operating unit, etc.) and the assessment results of the operating unit-designated implementation or testing responsibilities. If the AO determines that an acceptable level of risk exists when reusing an existing FedRAMP package or when issuing a DOC granted authorization and that the operating unit-level assessment results are acceptable, an authorization memorandum can be signed.

For DOC granted authorizations, OCRM in collaboration with the CSP uploads the entire authorization package, the FedRAMP checklist, and the signed authorization memorandum, in machine-readable and interoperable formats to the extent possible, to FedRAMP's Secure Repository and notifies the FedRAMP PMO at info@fedramp.gov.

After the FedRAMP PMO has reviewed the package and the CSP has addressed any technical issues, the FedRAMP PMO will publish the package on USDA Connect for other agencies to leverage. When an operating unit reuses an existing FedRAMP package, the operating unit must send its signed authorization memorandum to the FedRAMP PMO.

Cloud Continuous Monitoring Activities

In accordance with FedRAMP continuous monitoring requirements[23] and OMB M-24-15, a CSP must conduct continuous monitoring activities and submit deliverables (e.g., vulnerability scan results, POA&M report, waiver requests, change control logs[24], etc.) to the FedRAMP PMO at

[23] https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf

[24] Per OMB M-24-15, once a CSO is FedRAMP-authorized, CSPs are empowered to deploy changes and fixes to their products and services without requiring prior approval for individual changes. Per the revised guidance,

least monthly and on an as-needed basis after an authorization is granted. The FedRAMP PMO will then provide continuous monitoring data to federal agencies. This data will provide essential, near real-time security-related status information to assist the CSP and the DOC operating unit in taking appropriate risk remediation or mitigation actions, enabling the DOC operating unit to make cost-effective, risk-based decisions regarding the continued operation of the cloud information system. The DOC operating unit must review these materials to make risk-based decisions about ongoing authorization of the information system and obtain assurance regarding the security posture of the system for any authorization granted to a CSO as a part of continuous monitoring responsibilities.

In the event known vulnerabilities, incidents, or changes to the CSP pose a significant risk to the Department, operating unit, or mission, the SO is responsible for informing the AO and implementing risk mitigation measures, if possible. When all avenues to mitigate the risks, either by the CPO or the operating unit, have been exhausted without successful resolution, the AO may revoke the ATO and conduct analysis of alternatives to identify a replacement.

Customer-Responsible Controls

DOC SOs and ISSOs are responsible for conducting continuous monitoring activities for all customer-responsible controls and customer-managed POA&Ms, in accordance with the DOC ISCM Handbook.

Vulnerability and Risk Management

DOC operating units must adhere to the DOC ISCM Handbook and complete vulnerability scans of their PaaS and IaaS environments in accordance with the DOC VM Standard[25]. The CSP is responsible for conducting vulnerability scans for the CSO.

The extent of DOC responsibility for vulnerability scans varies with the cloud service model. For IaaS environments, the DOC retains responsibility for vulnerability scans for the information system and application on the cloud. For PaaS environments, the DOC retains responsibility for vulnerability scans for the DOC application hosted in the cloud. For SaaS environments, the CSP is responsible for completing vulnerability scans and the DOC is responsible for reviewing their vulnerability scan results.

Under OMB M-24-15, when the FedRAMP PMO becomes aware of significant vulnerabilities in a CSO with a FedRAMP authorization, the FedRAMP PMO will provide that information to the CSP and impacted agencies for remediation and may establish escalation pathways for vulnerabilities not addressed in a timely manner.

FedRAMP monitors the CSP's overall change process, rather than overseeing individual changes, and CSP change processes are addressed as part of FedRAMP continuous monitoring activities. Customers are responsible for reviewing CSP changes as part of their continuous monitoring activities and becoming aware of how the changes impact risks to the program and its data.

[25] Find Vulnerability Management Standard at Enterprise Cybersecurity Policy Program | Commerce Connection.

Emergency Directives and Binding Operational Directives

Under OMB M-24-15, the FedRAMP PMO is tasked with developing and maintaining procedures for responding to CISA BODs and EDs in an effort to centralize reporting processes, where feasible. However, individual agencies/customers remain responsible for continuously monitoring their CSPs responses and compliance with these directives to enable informed decision-making, particularly concerning incident response, risk mitigation, and contract/subscription renewals.

Annual Security and Privacy Control Assessment

The 3PAO for a CSP is required to complete annual assessments on a number of FedRAMP identified security controls. DOC operating units will assess controls that are the operating units' responsibility in accordance with the SPA&A Handbook. The AO has the option to vary the total number of controls tested by the 3PAO and can use the following criteria.

Table G-2: Annual Security and Privacy Control Assessment

Criteria		Description
1	Conditions from previous assessment	Any conditions made by the AO in the authorization letter or during a previous assessment. This includes the resolution of vulnerabilities within designated timeframes and implementation of new capabilities.
2	Weakness identified since the last assessment	Any area where the information system has known vulnerabilities or enhanced risk related to specific controls, such as an actual or suspected intrusion, compromise, malware event, loss of data, or denial of service (DoS) attack.
3	Known or suspected testing/continuous monitoring failure	Any area where the cloud system demonstrated a weakness or vulnerability in continuous monitoring or testing related to specific security controls, such as controls related to patch management, configuration management, or vulnerability scanning.
4	Control implementation that has changed since last assessment	Any control implementation that has changed since the last assessment must be independently assessed, even if it does not rise to the threshold of *significant change*.
5	Newly discovered vulnerability, zero-day attack, or exploit	Any control that is potentially affected by newly discovered vulnerabilities or zero-day exploits.
6	Recommendation of Authorizing Official or Organization	Based on direct knowledge and use of a cloud system, AOs or organizations can require the CSP to test additional controls based on unique mission concerns or based on the CSP's performance since their last assessment.

Incident Management

FedRAMP requires CSPs to report all incidents, and DOC operating units must be made aware of any incidents that occur regardless of whether they are directly impacted or have the potential to be impacted. DOC operating units are responsible for determining the extent of a confirmed or

suspected incident, surveying the impact, communicating findings to Enterprise Security Operations Center (ESOC), and if needed, initiating a response. DOC operating units must also ensure that CSPs report incidents according to the system's documented incident response plan. The following additional recommendations have been identified:

- CSPs may not notify the DOC if they do not confirm a suspected incident. As a countermeasure, DOC operating units should request that CSPs share incident reports quarterly to ensure the DOC is informed of early warning indicators and can take proactive action.
- DOC operating units should also establish a formal escalation process with CSPs to include a contact between both security operation center (SOC) teams
- DOC operating units should ensure data spill/unauthorized disclosure cleanup methods are incorporated into a Service Level Agreement (SLA).
- DOC operating units should ensure that the CSP IR plan is incorporated into the SLA, including communication plans, thresholds for reporting, requirement to comply with FedRAMP, and DOC IR processes and procedures, as defined in the DOC IRMS.

Disaster Recovery Procedures

DOC operating units should establish disaster recovery procedures to address recovery activities they may be responsible for when restoring cloud services quickly and effectively following a service disruption. Specifically, DOC operating units should at a minimum:

- Establish communication paths and methods
- Perform validation and functionality testing on an IaaS environment to verify that recovered data and configurations are correct and that the information system is ready to return to normal operations

Additional comprehensive procedures may be needed depending on the cloud service model and the tools available.

Cloud Service Provider Authorization Paths

Leveraging an existing FedRAMP agency or program authorization entails DOC operating units reusing an existing FedRAMP package to perform a quality and risk review of a CSP's CSO FedRAMP package from FedRAMP's secure repository, including its last ninety (90) day continuous monitoring deliverables, to implement and assess agency-specific controls in accordance with this guidance and the DOC SPA&A Handbook, and to issue an authorization memorandum. When a DOC operating unit grants an ATO, the DOC operating unit must notify OCRM and submit a copy of its ATO memorandum to the FedRAMP PMO.

In the event a CSO does not have a FedRAMP authorization, the DOC or an operating unit can grant its authorization upon validating the CSPs and its CSO's ability to meet FedRAMP and DOC-specific requirements. The DOC Office of the Chief Information (OCIO) supports the

successful execution of FedRAMP Agency ATOs for CSOs that DOC operating units are interested in adopting.

To ensure that secure and diverse CSOs are available to the DOC, the addition of CSOs should be prioritized based on the following prioritization criteria:

- CSO meets the definition of cloud computing as defined in NIST SP 800-145
- CSO is within scope of FedRAMP[26]
- Demonstrated demand for the CSO based on:
  - Current operating unit use
  - Potential operating unit use (projected adoption by the operating unit within 12 months)
  - Indirect Demand (a CSO depending on another CSO)
  - DOC policy & procedures, and/or OMB Memoranda requirements
- Ability to meet DOC SPCM and FedRAMP requirements
- CSP's ability to demonstrate a proven track record of managed risk and secure implementation
- Scheduled to obtain a FedRAMP agency authorization or program authorization
- Results of the readiness assessment report
- CSOs have partnered with a FedRAMP recognized 3PAO

The DOC Chief Information Officer (CIO) will serve as the AO for all DOC granted authorizations for enterprise wide CSOs. For CSOs used at operating unit-level, operating unit CIO or operating unit CISO may serve as the AO.

Initial Authorizing Agency Partnership

In order for a CSO to be considered for DOC or operating unit partnership, the requesting program office must complete and submit a formal request that addresses the following to OCRM, DOCITSecurity@doc.gov.

- Document the business/mission use case the CSO solves and anticipated end-user base
- Identify the 3PAO employed by the CSP that will complete the FedRAMP readiness assessment and full security assessment and provide their schedule to obtain FedRAMP authorization
- Indicate whether CSP accepts DOC partnership or initial FedRAMP agency authorization for its CSO
- Develop a project plan that maps out clear milestones associated with the operating unit-level authorization and deployment of the CSO

[26] OMB 24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*

- Identify the DOC operating unit project team members who will support the development, authorization, and operation of the CSO (e.g., SO, Project Manager, Information System Security Officer, Information System Engineers)

Evaluation Methodology

The DOC operating unit will engage with OCRM to have their request evaluated. This engagement will go through two stages of evaluation: prioritization criteria validation and final selection.

During the prioritization criteria validation phase, the operating unit presents the CSO request to OCRM. During this phase, OCRM evaluates the request and discusses the authorization process and requirements with the requesting operating unit. OCRM will also request access to and review the CSO readiness assessment report (RAR) to have a snapshot of the security posture of the CSO and its readiness for the authorization process. Additional information and meetings may be required as needed.

OCRM uses FedRAMP's Emerging Technologies Prioritization Framework[27], including its criteria and guidance[28], when developing prioritization characteristics for selected cloud services. These criteria are not mandatory for prioritization but are preferred characteristics and will be evaluated when the demand and a RAR does not provide a clear prioritization decision. During the final selection phase, OCRM consolidates the CSO requests, synopsis of the RAR and SPAR, and will take a decision on the CSP. OCRM will present the introduced/approved CSPs to the CIO council or CISO Council for situational awareness.

Issuing a FedRAMP Agency ATO

When a request is approved, the following activities must occur:

- The requesting DOC operating unit, in collaboration with OCRM, must complete a quality and risk review of the CSP's FedRAMP package to make an authorization recommendation to the AO. After briefing the AO and if an authorization is granted, OCRM will submit the authorization memorandum to the FedRAMP PMO.
- If an authorization is issued, the requesting DOC operating unit may move forward with completing their acquisition process. The requesting DOC operating unit must then complete operating unit-level assessment and authorization activities as defined in this document.

FedRAMP PMO Customer Success Team

The FedRAMP Agency Liaison Program establishes a voluntary community of trained individuals that will serve as a unified voice across Federal Agencies as they teach and facilitate FedRAMP processes and procedures. The FedRAMP PMO will develop and teach specialized training

[27] Emerging Technology Prioritization Framework | FedRAMP.gov

[28] Emerging Technologies Prioritization Criteria and Guidance V3 (FR Template)

material to the Agency Liaison cohort. Agency Liaisons will attend these training sessions and receive the materials and skills necessary to teach others within their Agency. Liaisons will also participate in forums developed to solicit feedback about the FedRAMP PMO and the services they offer.

DOC is represented by OCRM staff who participate in the Agency Liaison program to inform, enhance, and update Departmental policies, standards, and handbooks in alignment with FedRAMP policies and guidance.