IT Security Procedural Guide: Lightweight Security Authorization Process CIO-IT Security-14-68

Revision 8

September 13, 2024

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – November 3, 2014		
1	Bo Berlas	Added controls AC3 and AC6	Direction from CISO	Numerous
2	Bo Berlas	Lightweight ATO process templates added for systems operating in the CGI Federal IaaS Cloud	Provide coverage for systems hosted in the CGI Federal IaaS Cloud	Numerous
3	Bo Berlas	Guide updated to include process for initial authorizations.	Formalizes existing practice	Section 2 and 2.1
		Revision 2 – July 23, 2015		
1	Bo Berlas	Removed Static Code Analysis requirement	CISO direction	8, 13, and 16
2	Bo Berlas	Clarified Penetration Testing requirement	Updated to align with policy. For FIPS 199 Low and Moderate systems, penetration testing is performed for Internet accessible systems only.	8, 11, and 16
3	Bo Berlas	Updated templates to align with above changes	Aligns templates to updated requirements.	Appendices
		Revision 3 – August 19, 2016		
1	Wilson/ Klemens	Updated based on changes in GSA guidance and direction.	Removed IA-2(2) control, added CA-8(1) control	Multiple
		Revision 4 – November 3, 2016		
1	Klemens	Updated URLs, made formatting and minor editorial changes.	To update URLs for revised 90-day LATO Rules of Engagement Template and POA&M Template.	Multiple
		Revision 5 – February 6, 2017		
1	Klemens	Added information on the Sprint ATO process.	Update to reflect the newly defined Sprint ATO process.	Multiple
		Revision 6 – May 1, 2018		
1	Feliksa/ Klemens	Updated NIST SP 800-53 controls, consolidated control table into an Appendix, and integrated how the process relates to the NIST Cybersecurity.	Update to current GSA and Federal guidance and GSA requirements.	Throughout
		Revision 7 – September 15, 2021		
1	Dean/ Klemens	Updated to NIST SP 800-53, Revision 5 controls, added CA-7 and PL-2 controls. Updated requirements for the LATO process. Removed Sprint 90-day process.	Changes in the process and aligned with NIST SP 800-53, Revision 5 controls.	Throughout
		Revision 8 – September 13, 2024		
1	Klemens/ McCormick/ Normand	Revisions include: ● Added CISO approval required for all systems before following the lightweight security authorization process. ● Added RA-08 to the control set. ● Added Privacy controls for systems with PII. ● Moved ATO Package from Appendix A to Section 2.3.6 eliminating duplication. ● Editorial changes for clarity.	Changes in the process per GSA revised requirements.	Throughout

Approval

IT Security Procedural Guide: Title, CIO-IT Security 14-68, Revision 8, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

DocuSigned by:
Richard Speidel
171B5411103F48A...

Richard Speidel
GSA Chief Privacy Officer

The GSA OCISO and Privacy Program are independent organizations, staffed and funded separately, which develop and manage policies, processes, and procedures providing guidance and support in the implementation of security and privacy controls at GSA.

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov regarding security controls and this guide, and privacy.office@gsa.gov regarding privacy controls.

Table of Contents

1 Introduction 1
1.1 Purpose 4
1.2 Scope 4
1.3 References 4

2 Lightweight Security Authorization Process 6
2.1 Initial Steps 6
2.2 90-Day Limited Security Authorization Process 6
2.3 Full Lightweight Security Authorization Process 7
2.3.1 RMF PREPARE Step 7
2.3.2 RMF CATEGORIZE Step 8
2.3.3 RMF SELECT Step 9
2.3.4 RMF IMPLEMENT Step 10
2.3.5 RMF ASSESS Step 11
2.3.6 RMF AUTHORIZE Step 14
2.3.7 RMF MONITOR Step 16

Appendix A: Security and Privacy Controls for the Lightweight Security Authorization Process 19

Table 1-1: Lightweight ATO Process Table 1
Table 1-2. CSF Functions Mapped to NIST SP 800-37 RMF Steps 2
Table 2-1: Lightweight Security Authorization Process ATO Package 14

Note: Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Section 1.3. For example, Google Forms, Google Docs, and websites will have links.

1 Introduction

The General Services Administration (GSA) Lightweight Security Authorization Process results in an Authorization to Operate (ATO) for FIPS 199 Low and Moderate impact systems. During the ATO issued under the lightweight process the system is expected to pursue an ATO under one of GSA's other assessment and authorization (A&A) processes. The lightweight process is specific to **new** GSA applications residing on infrastructures that have a GSA ATO concurred by the GSA Chief Information Security Officer (CISO) or a Federal Risk and Authorization Management Program (FedRAMP) Infrastructure-as-a-Service (IaaS) ATO. Applications leveraging FedRAMP solutions must follow GSA's Leveraged FedRAMP SaaS solution process as described in CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk.

The GSA Lightweight Security Authorization Process facilitates rapid agile development and related assessment and authorization activities to more quickly bring systems into production following a risk-based approach. **Usage of the LATO process (90-Day, 1-Year Moderate, and 3-Year Low) is on an exception basis and requires GSA CISO approval by email to the IST and ISP Directors and the Chief Privacy Officer (CPO) based on a Security and Program Team presentation to the CISO on why a standard assessment and authorization to the full NIST 800-53 control baseline (by FIPS 199 impact level, as appropriate) cannot be achieved.**

The process in this guide allows Federal Information Processing Standards (FIPS) Publication (PUB) 199, "Standards for Security Categorization of Federal Information and Information Systems" Low and Moderate impact systems to be granted ATOs for the timeframes listed in Table 1-1 after completing the tailored National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) processes detailed in this guide.

Table 1-1: Lightweight ATO Process Table

ATO Attainable	Description
90-day Limited ATO (LATO) (FIPS 199 Low or Moderate)	A 90-day LATO is based on an external assessment consisting of: ● automated vulnerability and web application scanning ● automated and manual penetration testing (if Internet accessible).
One-year LATO (FIPS 199 Moderate)	A one-year LATO is based on completing all tasks in the Lightweight Security Authorization Process.
Three-year ATO (FIPS 199 Low)	A three-year ATO is based on completing all tasks in the Lightweight Security Authorization Process.

Note: During the time period of the ATO approved under this process, systems are to pursue an ATO under one of the other A&A processes identified in CIO-IT Security-06-30, resulting in a new ATO.

The lightweight security authorization process leverages the inherent flexibility in the application of security controls noted in NIST Special Publication (SP) 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," described as tailoring in NIST SP

800-37, Revision 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.” This approach has been used to align more closely with GSA processes (i.e., DevOps/SecDevOps and agile development) and environments of operation (i.e., environments that have a GSA ATO concurred by the GSA CISO or a FedRAMP ATO.) The process is focused on operational security from both a functional and assurance perspective and not on adherence to static checklists or the generating of large volumes of security authorization paperwork.

Executive Order (EO) 13800, “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” requires all agencies to use “The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the NIST or any successor document to manage the agency’s cybersecurity risk.” This NIST document is commonly referred to as the Cybersecurity Framework (CSF). The CSF complements, and does not replace, an organization’s risk management process and cybersecurity program. GSA uses NIST’s RMF as its foundation for managing risk. For more information on GSA’s alignment of the RMF to the CSF, refer to CIO-IT Security-06-30.

In support of EO 13800, GSA has aligned its risk management processes with the CSF. The five core CSF Functions are listed in the first column of Table 1-2. The second column lists the RMF Steps aligned with those CSF functions in the Lightweight Security Authorization Process. Details on the implementation of the RMF in this guide is provided in Section 2.3. For more information on GSA’s alignment of the RMF to the CSF, refer to CIO-IT Security-06-30.

Note: GSA is in the process of developing and updating CIO Order 2100.1, “Information Technology (IT) Security Policy'' to align to CSF 2.0, once that process is completed, the next version of this guide will align to CSF 2.0.

Table 1-2. CSF Functions Mapped to NIST SP 800-37 RMF Steps

CSF Function	Mapped RMF Steps
Identify (ID): Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	**Prepare** – Task P-18: System Registration **Categorize** – Task C-1, System Description – Task C-2, Security Categorization – Task C-3, System Categorization Review and Approval **Select** – Task S-1: Control Selection – Task S-5: Continuous Monitoring Strategy – System **Assess** – Task A-6: Plan of Action and Milestones **Authorize** – Task R-3: Risk Response **Monitor** – Task M-1: System and Environment Changes – Task M-2: Ongoing Assessments
Protect (PR): Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	**Select** – Task S-1: Control Selection **Implement** – Task S-1: Control Selection – Task S-1: Control Selection
Detect (DE): Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	**Select** – Task S-1: Control Selection – Task S-5: Continuous Monitoring - System **Monitor** Task S-1: Control Selection
Respond (RS): Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	**Select** – Task S-1: Control Selection **Monitor** – Task S-1: Control Selection
Recover (RC): Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	**Select** – Task S-1: Control Selection
No CSF Function Mapping	**Select** – Task S-6: Plan Review and Approval **Assess** – Task A-3: Control Assessments – Task A-4: Assessment Reports – Task A-5: Remediation Actions (Profile) **Authorize** – Task R-1: Authorization Package – Task R-2: Risk Analysis and Determination – Task R-4: Authorization Decision

1.1 Purpose

The purpose of this guide is to provide GSA's Federal employees and contractors a streamlined security authorization process that has tailored NIST SP 800-53, Revision 5 controls as described in NIST SP 800-37, Revision 2. The tailoring aligns the NIST SP 800-53 controls and NIST SP 800-37 A&A process more closely with GSA' processes (i.e., DevOps/SecDevOps and agile development) and environments of operation (i.e., environments that have a GSA ATO concurred by the GSA CISO or a FedRAMP ATO).

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who oversee/protect GSA information systems and data using the Lightweight Security Authorization Process. This guide is limited to systems that are:

- A **new** application in GSA;
- Resides on infrastructures that have a GSA ATO concurred by the CISO or a FedRAMP ATO; and
- Has obtained CISO approval prior to initiating the LATO process.

If a system does not meet the above criteria, one of the other A&A processes in CIO-IT Security-06-30 must be used.

1.3 References

Note: GSA updates its IT security policies and procedural guides on independent three-year cycles which may introduce conflicting guidance until revised guides are developed. In addition, many of the references listed are updated by external organizations which can lead to inconsistencies with GSA policies and guides. When conflicts or inconsistencies are noticed, please contact ispcompliance@gsa.gov for guidance.

Federal Laws, Regulations, and Guidance:

- CSF, Version 1.1, "Framework for Improving Critical Infrastructure Cybersecurity"
- EO 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems"
- NIST SP 800-30, Revision 1, "Guide for Conducting Risk Assessments"
- NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations"
- NIST SP 800-60, Volume I, Revision 1, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories"
- NIST SP 800-60, Volume II, Revision 1, "Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories"

- NIST SP 800-63 series, a set of four publications on Digital Identity Guidelines

GSA Guidance:

- CIO Order 1878.3, "Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices"
- GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy"

The procedural guides and templates below are referenced within the body of this guide and are available on the GSA.gov IT Security Procedural Guides page or on the internal IT Security Forms and Aids InSite page.

Guides:

- CIO-IT Security-01-05: Configuration Management (CM)
- CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk
- CIO-IT Security-04-26: Federal Information Security Modernization Act (FISMA) Implementation
- CIO-IT Security-08-39: FY24 IT Security Program Management Implementation Plan
- CIO-IT Security-09-44: Plan of Action and Milestones (POA&M)
- CIO-IT Security-11-51: Conducting Penetration Test Exercises
- CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program
- CIO-IT Security-18-91: Risk Management Strategy (RMS)
- CIO-IT Security-21-114: Clean Authorization to Operate (ATO) (in development)

Forms and Aids:

- FIPS 199 Low and Moderate versions of:
  - Lightweight Security Authorization SSPP Templates
  - Lightweight Authorization Process Control Implementation Summaries
  - GSA NIST 800-53 Rev5 LATO Test Case Workbooks
- FIPS 199 Security Categorization
- Digital Identity Acceptance Statement (DIAS)
- Security Assessment Plan (SAP)
- Security Assessment Report (SAR)
- POA&M Template
- Certification Letter
- ATO Letter

2 Lightweight Security Authorization Process

2.1 Initial Steps

Any information system under development or pursuing an ATO under an A&A process must determine:

(1) its FIPS 199 security categorization;
(2) if personally identifiable information (PII) is stored, processed, or transmitted; and
(3) the appropriate identity, authentication, and federation assurance levels (IAL, AAL, FAL) based on the NIST SP 800-63 series of documents.

These initial determinations, along with the criteria listed earlier, identify if a system is eligible to use the lightweight authorization process, if Privacy controls apply, and suitable methods for identity proofing and authentication. A brief description of these initial steps is provided below.

- **FIPS 199 Security Categorization.** The Lightweight Security Authorization Process is limited to FIPS 199 Low and Moderate systems and the criteria in Section 1.2. The security categorization process described under Task C-2 is used to determine a system's FIPS 199 level.
- **Privacy Threshold Assessment (PTA)/Privacy Impact Assessment (PIA).** GSA Order CIO 1878.3, "Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices," provides guidance on completing PTAs and PIAs. The program and policy require developing PTAs, and PIAs when applicable, to identify PII before the development or acquisition of a new information system.
- **DIAS.** The GSA DIAS template aids the system owner and security personnel in determining the levels of assurance regarding digital identities required for a system. When completed, it identifies the digital identity proofing, authentication, and federation (if applicable) methods suitable for the system.

2.2 90-Day Limited Security Authorization Process

The 90-day Limited Security Authorization Process is available to systems at the FIPS 199 Low and Moderate levels. The 90-day Limited ATO is based upon a security assessment consisting of external vulnerability and web application scanning (as applicable) and penetration testing. The assessment includes the following activities:

- Review and approval of the information system's architecture by the OCISO Security Engineering Division (ISE)
- Development of a FIPS 199 Security Categorization Template
- Development of a PTA, and PIA (if applicable)
- Development of a DIAS
- Completion of Unauthenticated external vulnerability scanning
- Completion of Unauthenticated external web application scanning
- Completion of External Gray-box penetration testing

External vulnerability and web application scanning will be conducted by the OCISO ISO Division while Penetration Testing will be conducted by the OCISO IST Division. The vulnerability scanning and penetration test, and a Penetration Test Report, will be completed within two (2) weeks of approval of the system's assessment rules of engagement (RoE).

Any Very High/Critical or High vulnerabilities identified during assessment activities must be fixed or mitigated prior to a 90-day Limited ATO approval. When Very High/Critical or High vulnerabilities are identified during the assessment activities, every effort will be made to re-assess those vulnerabilities to verify that implemented mitigation strategies have adequately reduced the associated risks.

Note: If the system is not ready for assessment with sufficient time for re-assessment within the two-week period, the test report will be issued "as is."

The following documents, except for the Penetration Test Report, will be prepared by the supporting ISSO to form the basis for the 90-day Security Authorization Package:

- Architecture review conducted by ISE
- FIPS 199 Security Categorization
- PTA/PIA
- DIAS
- Vulnerability Scan Results
- Penetration Test Report
- POA&M
- Certification Memo
- ATO Letter

A 90-day LATO must not be extended. During its 90-day LATO, a system must complete the full lightweight authorization process described in Section 2.3 to achieve:

(1) A three-year ATO if the system is FIPS 199 Low.
(2) A one-year LATO if the system is FIPS 199 Moderate.

One of the criteria for using the lightweight process is that a system is a **new** GSA system, therefore all systems using the process must receive its next ATO by following one of the other A&A processes defined in CIO-IT Security-06-30.

2.3 Full Lightweight Security Authorization Process

The key activities in the Lightweight Security Authorization Process and its implementation of the NIST RMF are detailed in the following subsections.

2.3.1 RMF PREPARE Step

From NIST SP 800-37, "The purpose of the Prepare step is to carry out essential activities at the organization, mission and business process, and information system levels of the

organization to help prepare the organization to manage its security and privacy risks using the Risk Management Framework."

Task P-18: System Registration - Program Managers and Project Managers collaborate with the GSA Services and Staff Offices (SSO) as new systems are being considered for design, development, piloting, or implementation. GSA's Information System Security Managers (ISSMs) and ISSOs work closely with those offices and personnel to ensure systems are registered into the GSA system inventory as early as possible. GSA's governance, risk, and compliance (GRC) tool is the repository for GSA's system inventory. Systems are registered in it as soon as they are identified and categorized as pending. They remain in this status until they are placed into production. Systems following the process in this guide will be identified in GSA's GRC tool accordingly.

2.3.2 RMF CATEGORIZE Step

From NIST SP 800-37, "The purpose of the Categorize step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems."

TASK C-1: System Description - The information system is described throughout Sections 1-12 of the SSPP template. The system owner, in collaboration with the ISSO, completes these sections of the system's SSPP. The sections cover the system's:

- operational environment,
- hardware and software inventory,
- FIPS 199 security categorization,
- data, users,
- roles,
- architecture,
- connections,
- etc.

Each section should be sufficiently detailed to permit readers to understand the:

- business functions of the system,
- how the system architecture and components support those functions,
- how data is collected, processed, and transmitted internally and externally (i.e., data flow),
- sensitivity of the data the system handles,
- user base, and
- key points of contact.

TASK C-2: Security Categorization - Use GSA's FIPS 199 Security Categorization Template to identify the information types handled by the system. NIST SP 800-60 Volumes I and II are used to identify the information types handled by the system. The data owner collaborates with the System Owner and the ISSO to complete the template. Once completed the system's security categorization is summarized in the SSPP with the completed template attached to the system's SSPP.

Task C-3: System Categorization Review and Approval - The system FIPS 199 security categorization from the previous step must be reviewed and approved by the AO, CISO, and Senior Agency Official for Privacy (SAOP), or their designated representatives. Delegated representatives must be Federal employees. The ISSO collaborates with the AO, OCISO, Privacy Team, and data owner as necessary to have the FIPS 199 security categorization approved.

2.3.3 RMF SELECT Step

From NIST SP 800-37, "The purpose of the Select step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation."

Task S-1: Control Selection - The security controls required for the Lightweight Security Authorization Process are identified in Appendix A. The Lightweight Security Authorization Process tailored baseline can be supplemented with additional controls and/or control enhancements, as necessary, to address unique organizational and/or system specific needs based on a risk assessment (either formal or informal) and local conditions including:

- environment of operation,
- organization-specific security requirements,
- specific threat information,
- cost-benefit analyses, or
- special circumstances.

Additional controls are at the discretion of the CISO and AO in coordination with the ISSM, ISSO, System Owner, and Privacy Team as necessary.

Document the selected security controls, including any controls or enhancements selected above the baseline for the information system, in the Lightweight Security Authorization Process SSPP template available on the IT Security Forms and Aids InSite page.

Task S-5: Continuous Monitoring Strategy – System - Systems must develop a system-level strategy for monitoring its security controls. The system-level strategy must align with the RMF Monitor Step, CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program, and CIO-IT Security-08-39: FY24 IT Security Program Management Implementation Plan. The system-level strategy must address monitoring of controls that are not monitored as part of GSA's ISCM strategy and the frequency of control monitoring. It defines how system changes are monitored, how risk is assessed, and how monitoring results are reported. The System Owner collaborates with the ISSM, ISSO, the Privacy Team as necessary, and others to establish the system-level continuous monitoring strategy.

Task S-6: Plan Review and Approval – The system SSPP must be reviewed and approved. The System Owner collaborates with the ISSM, ISSO, Data Owners, the Privacy Team as necessary, and other System Owners (regarding common/hybrid controls), and others to complete the SSPP, including appendices and attachments.

For new systems under development, note that in the Select Step implementation details may not be fully described since the exact implementation to satisfy control requirements may not be complete. Once completed, the SSPP is signed by the System Owner, ISSO, and the ISSM. As

applicable the SSPP is signed by the Vendor ISSO assigned to the system. The SSPP and its appendices/attachments must be updated and completed as the security controls are implemented in the RMF Implement Step.

Note: Approving the SSPP via the signatures noted is an agreement that the set of security controls (system-specific, hybrid, and/or common controls) proposed to meet the security requirements for the information system are sufficient. This approval allows the next step in the RMF to commence (i.e., the implementation of the security controls).

The ISE Division must review and approve the Security Architecture before the system's security controls are implemented.

2.3.4 RMF IMPLEMENT Step

From NIST SP 800-37, "The purpose of the Implement step is to implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation."

Task I-1: Control Implementation - Describe the security and privacy control implementation details in the SSPP; providing a functional description of how the control is satisfied. Security control implementation should be consistent with the GSA enterprise architecture and information security architecture. IT systems shall be configured and hardened using GSA IT security hardening guidelines (i.e., security benchmarks), NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as deemed appropriate by the AO.

To the greatest extent possible, systems are encouraged to conduct initial security control assessments (also referred to as developmental testing and evaluation) during information system development and implementation. Such testing, conducted in parallel with the development and implementation of the system, facilitates the early identification of weaknesses and deficiencies and provides the most cost-effective method for initiating corrective actions.

Systems leveraging a cloud solution must implement the customer responsibilities identified in the Cloud Service Provider's (CSP's) Customer Responsibility Matrix (CRM). Only customer responsibilities associated with NIST controls in the system's FIPS 199 control baselines must be addressed. For example, if a system is FIPS 199 Low and the CSP CRM includes FIPS 199 Moderate controls only the FIPS 199 Low controls will be addressed (and GSA OCISO specified controls, as necessary).

Federal requirements, such as CISA Cybersecurity Directives, include specific implementation instructions which must be adhered to in order to secure the system and comply with the requirements.

The security control implementation descriptions must include planned inputs, expected behavior, and expected outputs (where appropriate) that are typical for technical controls. The SSPP must also address platform dependencies and include any additional information necessary to describe how the security capability required by the security control is achieved at the level of detail sufficient to support a control assessment in Task A-3.

Security controls are documented in Section 13 of the SSPP. This section must provide a thorough description of how the LATO security and privacy controls for the system are being implemented or planned to be implemented. Detailed instructions for completing the SSPP are

in the template available on the GSA IT Security Forms and Aids Insite page. For each control, descriptions must:

- Describe how (including what, when, where, and who) the security control is being implemented or planned to be implemented for all parts of the control;
- Identify any scoping guidance that has been applied;
- Explain how all specified parameters have been met (i.e., not just stating they have been met, describe *how* they are met);
- Establish time-bound plans for planned controls;
- Provide a rationale and supporting evidence for any controls identified as Not Applicable;
- Describe control implementations across all components/subsystems for systems with multiple components or subsystems; and
- Describe how the customer responsibilities in the CSP's CRM are implemented for systems leveraging a cloud solution.

Systems leveraging a cloud solution must implement the customer responsibilities identified in the CSP's CRM. Only customer responsibilities associated with NIST controls in the system's FIPS 199 control baselines must be addressed. For example, if a system is FIPS 199 Low and the CSP CRM includes FIPS 199 Moderate controls only the FIPS 199 Low controls will be addressed (and GSA OCISO specified controls, as necessary).

The System Owner collaborates with the ISSM, ISSO, Privacy Team as necessary, other System Owners (regarding common/hybrid controls), and others to complete all control implementations in the SSPP.

Task I-2: Update Control Implementation - During development, or while operating and maintaining the system, the implementation details of controls may change. Changes occur for many reasons, including, but not limited to, infeasibility of the design, new capabilities being made available, patches and upgrades to the system. The SSPP must be updated to reflect any changed implementation details so the SSPP always reflects the "*as implemented*" state of the system. In this manner when assessments in the next RMF step occur the assessors can determine if the system reflects its documented state or there are inconsistencies that need to be rectified.

The System Owner collaborates with the ISSM, ISSO, Privacy Team as necessary, other System Owners (regarding common/hybrid controls), and others to update control implementations in the SSPP as necessary.

2.3.5 RMF ASSESS Step

From NIST SP 800-37, "The purpose of the Assess step is to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization."

The following tasks detail the actions in the RMF Assess Step. As GSA implements automation into its A&A processes, the tasks described in the following sections will be migrated, as much as possible, to GSA's GRC tool implementation.

Task A-2: Assessment Plan - Assessors must develop and obtain approval of a Security Assessment Plan (SAP) which will be leveraged to assess the security controls of the system. The SAP provides system background information, the objectives for the security control assessment, the assessment approach, and the assessment test cases to be used in Task A-3. Developing the plan may require updates and/or supplements to GSA's NIST 800-53 Revision 5 LATO Test Cases. As necessary assessors will incorporate additional assessment test cases for any supplemented controls and/or control enhancements added during the RMF Select step.

The SAP must be reviewed and approved by the ISSO and ISSM to ensure the plan:

- includes all appropriate security controls;
- is consistent with system/organizational security objectives;
- employs required assessment tools and techniques;
- provides assessment test cases; and
- defines the scope of the assessment and any conditions or restrictions.

The overall purpose of the SAP approval is two-fold: (1) to establish the appropriate expectations for the security control assessment; and (2) to bound the level of effort for the security control assessment.

Task A-3: Control Assessments - Assessors assess the security controls using the LATO Test Cases, including any supplemental or updated tests based on the specific system (e.g., assessing BODs or other Federal requirements). The assessment determines if the controls implemented in the RMF Implement Step are operating as intended and producing the desired outcome with respect to meeting the security requirements for the information system. Systems leveraging cloud solutions must include assessing the implementation of customer responsibilities from a CSP's CRM in the assessment.

Appendix A identifies the security controls requiring assessment.

The following sections further define GSA's scanning and penetration testing types.

Configuration Settings - Operating System Configuration Analysis

Security configuration analysis is performed by the ISO Division and/or the contractor organization supporting the information system (as per contract). For GSA Enterprise Cloud Environments supported by the OCISO, the ISO Division will be able to support configuration scanning; for other environments, the supporting infrastructure/application development team will be responsible for instantiating a vulnerability scanning solution and the performance of necessary configuration scanning.

Configuration scanning will be performed as an authenticated scan using a combination of automated scanning tools (e.g., Tenable), and manual review. For cloud environments such as AWS, the authenticated scan must be conducted from within the Virtual Private Cloud (VPC) supporting the information system to allow full access to all server settings and configurations. Configuration scans must align with the related GSA or CIS benchmark used to harden and configure the server(s).

Vulnerability Scanning

Operating System Vulnerability Scan
Operating system vulnerability scanning will be performed by the ISO Division Scan Team and/or the contractor organization supporting the information system (as per contract). For GSA Enterprise Cloud Environments supported by the OCISO, the ISO Division Scan Team will be able to support vulnerability scanning; for other environments, the supporting infrastructure/application development team will be responsible for instantiating a vulnerability scanning solution and the performance of necessary vulnerability scanning.

Vulnerability scanning will be performed as an authenticated scan using a combination of automated scanning tools (e.g., Tenable), and manual review. For cloud environments, the authenticated scan shall be conducted from within the CSP's firewall to allow full access to all server settings and configurations. For systems with databases, the scanning tool must be configured to include any applicable database checks,

Web Application Vulnerability Scan
Web application vulnerability scanning will be performed by the ISO Division Scan Team and/or the contractor organization supporting the information system (as per contract). Testing is performed from external scanning systems against the information system using a variety of automated (e.g., Invicti) and manual scanning tools. The main purpose of the Web Application Vulnerability Scan is to discover and enumerate any deficiencies in the exposed web interface that could be leveraged by an attacker to gain access to unauthorized systems or data. Web application scanning will focus on the latest version of the Open Web Application Security Project (OWASP) Top Ten security risks to web applications.

CA-8 Penetration Testing

Penetration testing will be performed for all Internet-accessible information systems. Penetration testing will be performed by the IST Division in accordance with CIO-IT Security-11-51: Conducting Penetration Test Exercises.

TASK A-4: Assessment Reports – Assessors prepare a SAR documenting the issues, findings, and recommendations of the security control assessment (including, if applicable, a penetration test report as an attachment). The SAR documents the assessment findings with recommendation(s) and risk determinations based on NIST SP 800-30 Revision 1. Multiple findings regarding the SSPP (Control PL-2) can be consolidated into one finding and associated with PL-2. All other findings rated Moderate and above are reported individually in the SAR.

Additional information on addressing findings based on the source of the findings (e.g., test cases, scans, pen tests) is provided in the SAR template available on the GSA IT Security Forms and Aids Insite page. The SAR will be included as part of the authorization package.

TASK A-5: Remedial Actions - Systems may perform initial remediation actions on security controls based on the findings and recommendations of the SAR and have the assessors reassess remediated control(s), as appropriate. Assessors should identify remediated vulnerabilities as "Remediated" in the final SAR. Similarly, any findings proven to be a false positive should be identified as "False Positive."

Additional instructions are provided in the SAR template. The assessors, in coordination with the System Owner, ISSO, and other system personnel, validate remediated and false positive findings.

TASK A-6: Plan of Action and Milestones - A system's POA&M describes how the System Owner intends to address identified risks (i.e., reduce, eliminate, or mitigate risks). A POA&M Template and details on developing POA&Ms are contained in the CIO-IT Security-09-44: Plan of Action and Milestones (POA&M). A GSA POA&M Template is available on the IT Security Forms and Aids web page. POA&M assistance is available by contacting ispcompliance@gsa.gov.

GSA tracks all POA&Ms on POA&M Shared Drives which serve as the primary tool for the management, storage, and dissemination of GSA system and program POA&Ms. GSA will be implementing POA&Ms in its GRC tool in the future. As systems' POA&Ms are migrated into the GRC tool, they will be tracked in it.

The ISSO collaborates with the System Owner, other system personnel, and the ISSM and creates POA&Ms as described in the following sections.

2.3.6 RMF AUTHORIZE Step

From NIST SP 800-37, "The purpose of the Authorize step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable."

TASK R-1: Authorization Package – The ISSO assembles the security authorization package. Table 2-1 lists the documents required for Lightweight Security Authorization Packages. Templates for the documents listed (unless otherwise noted) are available on the GSA IT Security Forms and Aids Insite page.

POA&Ms must reside on the POA&M Team Drive for the system.

Table 2-1: Lightweight Security Authorization Process ATO Package

Description
90-Day LATO
Architecture review conducted by ISE (ISE prepares/not on InSite)
FIPS 199 Security Categorization
PTA/PIA
DIAS
Vulnerability Scan Results (ISO provides/not on InSite)
Penetration Test Report
POA&M
Certification Letter
ATO Letter
One Year LATO and Three Year ATO
SSPP (with appendices/attachments) Appendix A - References Attachment 1: PTA/PIA Attachment 2: FIPS 199 Security Categorization Attachment 3: DIAS Attachment 4: Code Review Report Attachment 5: Penetration Test Results (if applicable) Attachment 6: Vulnerability Scan Results
SAR (with appendices/attachments)

Description
Appendix A - Acronyms Attachments: Additional Supporting Documents (as necessary)
CRM - Please contact the designated ISSM to receive the vendor's current CRM for the system.
POA&M
Certification Letter
ATO Letter

TASK R-2: Risk Analysis and Determination - The AO makes the risk-level determination. To do so, the AO assesses all the information documented in the Security Authorization Package regarding the current security state of the system or the common controls inherited by the system and the recommendations for addressing any residual risks. The AO consults with the CISO, System Owner, ISSM, ISSO, and others as necessary, to determine if the package provides enough information to establish a credible level of risk.

TASK R-3: Risk Response - The AO consults with the CISO, System Owner, ISSM, ISSO, SAOP and CPO (for systems that have a PIA), and others as necessary, to determine if the residual risks in operating the system need to be mitigated or can be accepted and managed via POA&Ms prior to authorization. As part of risk response, POA&Ms can be prioritized, based on risk or other factors, to focus resources on the POA&Ms that will have the greatest impact in reducing risk.

Task R-4: Authorization Decision – The explicit acceptance of risk is the responsibility of the AO. The AO determines if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable. The AO must consider many factors, balancing security considerations with mission and operational needs. The AO issues an authorization decision for the information system and the common controls inherited by the system after reviewing all the relevant information. The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the risk to the agency is acceptable.

The preparation and routing for review and signature of the system's authorization package is summarized as follows:

- IST quality checks and validates the package and prepares a Certification Letter and uploads documents to Archer GRC (if not already uploaded).
- ISP reviews Archer GRC to ensure the entire package is present, then reviews the package for completeness and consistency.
- ISP coordinates with the ISSM on the preparation of the ATO Letter and uploads it to Docusign.
- The CISO reviews the package and coordinates with the ISSM and others and signs the letter (or directs changes).
- The AO is briefed and base on the evidence provided and whether it establishes an acceptable risk decides to:
  - Authorize system operation without any restrictions or limitations on its operations.
  - Authorize system operation with restrictions/limitations on its operations. The POA&M must include detailed actions to correct the deficiencies requiring the

restrictions/limitations. The ISSM/ISSO must resubmit an updated authorization package upon completion of required POA&M actions to move to a full ATO without any restrictions/limitations.
- Not authorize the system for operation.

2.3.7 RMF MONITOR Step

From NIST SP 800-37, “The purpose of the Monitor step is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions.”

The following tasks detail the actions in the RMF Monitor Step. As GSA implements automation into its A&A processes, the tasks described in the following sections will be migrated, as much as possible, to GSA’s GRC tool.

Task M-1: System and Environment Changes - System Owners must determine the security impact of proposed or actual changes to the information system and its operational environment. Per CIO-IT Security-01-05: Configuration Management (CM), proposed system changes must be evaluated to determine potential security impacts. An impact analysis of each proposed change will be conducted using the following as a guideline:

- Whether the change is viable and improves the performance or the security of the system;
- Whether the change is technically correct, necessary, and feasible within the system constraints;
- Whether system security will be affected by the change;
- Whether associated costs for implementing the change were considered; and
- Whether security components are affected by the change.

As outlined within CIO-IT Security-18-91: Risk Management Strategy (RMS), GSA has a rigorous configuration change management process. It states:

- Any IT changes are requested through a defined CM approval process (e.g., a chartered Configuration Control Board [CCB]) using automated or manual processes to document the:
  - nature of changes,
  - their criticality,
  - impacts on the user community,
  - testing and rollback procedures,
  - stakeholders, and
  - points of contact.
- System changes are tested and validated prior to implementation into the production environment.
- Configuration settings and configuration baselines are updated as necessary to meet new technical and/or security requirements and are controlled through the CM process.

- The CM process requires testing/validating changes where the scope of the change has a major impact on agency reputation, has a large scope or has the potential for significant monetary impact.

Changes may be required by outside influences. For example, if a successful exploit or identified vulnerability can be resolved or mitigated by configuration or process changes, the same CM process described above must be followed to ensure the resolution does not have unintended consequences.

Task M-2: Ongoing Assessments - System Owners are responsible for assessing a subset of the NIST SP 800-53 security controls employed within and inherited by the information system in accordance with GSA's monitoring strategy. Per CIO-IT 01-05, the implemented CM process calls for continuous system monitoring to ensure that systems are operating as intended and that implemented changes do not adversely impact either the performance or security posture of the systems. Per CIO-IT Security-04-26, GSA's annual Federal Information Security Modernization Act (FISMA) self-assessments will assess a subset of security controls. Controls are selected based on an analysis of:

- past audit findings,
- known weaknesses or controls that have resulted in security breaches,
- key controls (e.g., showstopper controls, critical controls), and
- volatile controls that should be assessed frequently.

Ongoing assessments include penetration tests and OIG audits that are performed on systems.

GSA conducts ongoing assessments by leveraging its deployment of Continuous Diagnostics and Mitigation (CDM) and other enterprise security management tools. GSA's tool stack facilitates the ongoing assessments of GSA information systems by performing vulnerability scans and checking the configuration settings of systems against GSA required hardening benchmarks.

Task M-4: Authorization Package Updates - The System Owner and ISSO will update the following items as part of the system and GSA continuous monitoring plans, processes, and program:

- SSPP (and all appendices and attachments)
- POA&M

The updates will be based on regular updates required by GSA processes, such as:

- Vulnerability scans from GSA's scanning program;
- Annual FISMA self-assessments;
- Penetration tests;
- Audits, or related assessments; and
- Changes identified as part of a system's CM Plan.

As part of the CM process outlined within CIO-IT Security-01-05, security testing will be conducted following major or significant system changes. If the changes introduce vulnerabilities, actions to mitigate the vulnerabilities must be included in the system's POA&M, per GSA's POA&M management process, for tracking of the resolution. The system's SSPP will be updated to reflect any changes.

Appendix A: Security and Privacy Controls for the Lightweight Security Authorization Process

A security control test case must be completed for each control in the table below using the templates identified in Appendix A. The ISSO Support Division (IST) is responsible for ensuring all the security and privacy controls are assessed. The legend below provides important information concerning the highlighting used in the control table. If scanning cannot be performed by the ISO division, IST is responsible for ensuring equivalent scanning is performed.

Legend	
	ISO Division - Performs Vulnerability and Configuration/Compliance scanning, where possible.
	ISE Division - Performs security architecture review.
	Only required for Internet accessible systems, performed by IST Division.
	Only required for systems with Personally Identifiable Information.

800-53 Control	Control Title
AC-02	Account Management
AC-03	Access Enforcement
AC-03(14)	Access Enforcement | Individual Access
AC-06(05)	Least Privilege | Privileged Accounts
AC-06(09)	Least Privilege | Log Use of Privileged Functions
AT-03(05)	Role-based Training | Processing Personally Identifiable Information
AU-02	Event Logging
AU-03(03)	Content of Audit Records | Limit Personally Identifiable Information Elements
AU-06(01)	Audit Record Review, Analysis, and Reporting | Automated Process Integration
CA-07	Continuous Monitoring
CA-08	Penetration Testing
CM-02(02)	Baseline Configuration | Automation Support for Accuracy and Currency
CM-03(01)	Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes
CM-06(01)	Configuration Settings | Automated Management, Application, and Verification
CM-07(05)	Least Functionality | Authorized Software - Allow-By-Exception
CM-08(02)	System Component Inventory | Automated Maintenance
CP-07(01)	Alternate Processing Site | Separation from Primary Site
IA-02	Identification and Authentication (Organizational Users)
IA-02(01)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts
IA-02(02)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts
IR-02(03)	Incident Response Training | Breach
IR-08(01)	Incident Response Plan | Breaches
MP-06	Media Sanitization
PL-02	System Security and Privacy Plans
PL-08	Security and Privacy Architectures
PT-02	Authority to Process Personally Identifiable Information

PT-03	Personally Identifiable Information Processing Purposes
PT-04	Consent
PT-05	Privacy Notice
PT-05(02)	Privacy Notice | Privacy Act Statements
PT-06	System of Records Notice
PT-06(01)	System of Records Notice | Routine Uses
PT-06(02)	System of Records Notice | Exemption Rules
PT-07	Specific Categories of Personally Identifiable Information
PT-07(01)	Specific Categories of Personally Identifiable Information | Social Security Numbers
PT-07(02)	Specific Categories of Personally Identifiable Information | First Amendment Information
PT-08	Computer Matching Requirements
RA-05	Vulnerability Monitoring and Scanning
RA-08	Privacy Impact Assessments
SA-08(33)	Security and Privacy Engineering Principles | Minimization
SA-11(01)	Developer Testing and Evaluation | Static Code Analysis
SA-22	Unsupported System Components
SC-07	Boundary Protection
SC-07(24)	Boundary Protection | Personally Identifiable Information
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection
SC-28(01)	Protection of Information at Rest | Cryptographic Protection
SI-02	Flaw Remediation
SI-04	System Monitoring
SI-04(02)	System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis
SI-04(04)	System Monitoring | Inbound and Outbound Communications Traffic
SI-04(05)	System Monitoring | System-Generated Alerts
SI-07	Software, Firmware, and Information Integrity
SI-10	Information Input Validation
SI-12(01)	Information Management and Retention | Limit Personally Identifiable Information Elements
SI-12(02)	Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research
SI-18	Personally Identifiable Information Quality Operations
SI-18(04)	Personally Identifiable Information Quality Operations | Individual Requests
SI-19	De-identification