



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

**Revision 7**

September 17, 2021


*Office of the Chief Information Security Officer*

**VERSION HISTORY/CHANGE RECORD**

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
<b>Revision 1 – November 3, 2014</b>				
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
<b>Revision 2 – July 23, 2015</b>				
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
<b>Revision 3 – August 19, 2016</b>				
1	Wilson/ Klemens	Updated based on changes in GSA guidance and direction.	Removed IA-2(2) control, added CA-8(1) control	Multiple
<b>Revision 4 – November 3, 2016</b>				
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
<b>Revision 5 – February 6, 2017</b>				
1	Klemens	Added information on the Sprint ATO process.	Update to reflect the newly defined Sprint ATO process.	Multiple
<b>Revision 6 – May 1, 2018</b>				
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
<b>Revision 7 – September 17, 2021</b>				
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

## **Approval**

IT Security Procedural Guide: Title, CIO-IT Security 14-68, Revision 7, is hereby approved for distribution.

DocuSigned by:  
  
FD717926161544F...

---

Bo Berlas  
GSA Chief Information Security Officer

**Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at [ispcompliance@gsa.gov](mailto:ispcompliance@gsa.gov).**

## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Purpose .....	3
1.2	Scope.....	3
1.3	References .....	3
<b>2</b>	<b>Lightweight Security Authorization Process .....</b>	<b>5</b>
2.1	Initial Steps.....	5
2.2	90-Day Limited Authorization.....	5
2.3	One-Year Limited ATO for FIPS 199 Moderate and Three-Year ATO for FIPS 199 Low Impact Systems.....	6
2.3.1	RMF PREPARE Step .....	7
2.3.2	RMF CATEGORIZE Step .....	7
2.3.3	RMF SELECT Step .....	8
2.3.4	RMF IMPLEMENT Step.....	9
2.3.5	RMF ASSESS Step .....	10
2.3.6	RMF AUTHORIZE Step.....	13
2.3.7	RMF MONITOR Step.....	14
	<b>Appendix A: Lightweight Security Authorization ATO Package.....</b>	<b>17</b>
	<b>Appendix B: Security Controls for the Lightweight Security Authorization Process .....</b>	<b>18</b>

## List of Tables

<b>Table 1-1: Lightweight ATO Process Table.....</b>	<b>1</b>
<b>Table 1-2: CSF Functions Mapped to NIST SP 800-37 RMF Steps.....</b>	<b>2</b>
<b>Table A-1: Lightweight Security Authorization Process ATO Package.....</b>	<b>17</b>

### Notes:

- 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 webpage or document listed in [Section 1.3](#). For example, Google Forms, Google Docs, and websites will have links.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

## 1 Introduction

The General Services Administration (GSA) Lightweight Security Authorization Process is specific to new GSA applications residing on infrastructures that have a GSA Authorization to Operate (ATO) concurred by the GSA Chief Information Security Officer (CISO) or a Federal Risk and Authorization Management Program (FedRAMP) Infrastructure-as-a-Service (IaaS) provisional ATO. Applications leveraging FedRAMP SaaS or PaaS solutions must follow GSA's Leveraged FedRAMP XaaS solution process as described in CIO-IT Security-06-30, "Managing Enterprise Cybersecurity Risk." Exceptions to the above must be approved by GSA CISO and AO.

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
<b>90-day Limited ATO (LATO) (FIPS 199 Low or Moderate)</b>	A 90-day LATO is based on an external assessment including automated vulnerability and web application scanning as well as automated and manual penetration testing (if Internet accessible). Eligibility to pursue a 90-day LATO is determined on a case-by-case basis and must be approved by the GSA CISO and AO.
<b>One-year LATO (FIPS 199 Moderate)</b>	A one-year LATO is based on completing all tasks in the Lightweight Security Authorization Process (see <a href="#">Section 2.4</a> ).
<b>Three-year Full ATO (FIPS 199 Low)</b>	A three-year authorization based on completing all tasks in the Lightweight Security Authorization Process (see <a href="#">Section 2.4</a> ).

**Note:** For FIPS 199 Moderate information systems, the one-year limited ATO is to be used to conduct a full security assessment and authorization (A&A) consistent with requirements 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 and agile development) and environments of operation (i.e., environments that have a GSA ATO concurred by the GSA CISO or a FedRAMP IaaS provisional 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), 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 the CSF functions in the Limited Authorization to Operate (LATO) process. Details on the implementation of the RMF in the Lightweight Security Authorization Process is provided in [Section 2.4](#). For more information on GSA’s alignment of the RMF to the CSF, refer to CIO-IT Security-06-30.

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

CSF Function	Mapped RMF Steps
<p><b>Identify (ID):</b> Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.</p>	<p><b>Prepare</b> – Task P-18: System Registration</p> <p><b>Categorize</b> – Task C-1, System Description – Task C-2, Security Categorization – Task C-3, System Categorization Review and Approval</p> <p><b>Select</b> – Task S-1: Control Selection – Task S-5: Continuous Monitoring Strategy – System</p> <p><b>Assess</b> – Task A-6: Plan of Action and Milestones</p> <p><b>Authorize</b> – Task R-3: Risk Response</p> <p><b>Monitor</b> – Task M-1: System and Environment Changes – Task M-2: Ongoing Assessments</p>
<p><b>Protect (PR):</b> Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.</p>	<p><b>Select</b> – Task S-1: Control Selection</p> <p><b>Implement</b> – Task S-1: Control Selection – Task S-1: Control Selection</p>
<p><b>Detect (DE):</b> Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.</p>	<p><b>Select</b> – Task S-1: Control Selection – Task S-5: Continuous Monitoring - System</p> <p><b>Monitor</b> Task S-1: Control Selection</p>
<p><b>Respond (RS):</b> Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.</p>	<p><b>Select</b> – Task S-1: Control Selection</p> <p><b>Monitor</b> – Task S-1: Control Selection</p>

CSF Function	Mapped RMF Steps
<b>Recover (RC):</b> 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.	<b>Select</b> – Task S-1: Control Selection
<b>No CSF Function Mapping</b>	<b>Select</b> – Task S-6: Plan Review and Approval <b>Assess</b> – Task A-3: Control Assessments – Task A-4: Assessment Reports – Task A-5: Remediation Actions (Profile) <b>Authorize</b> – Task R-1: Authorization Package – Task R-2: Risk Analysis and Determination – Task R-4: Authorization Decision

## 1.1 Purpose

This procedural guide defines a lightweight security authorization process for systems meeting the following criteria and completing the appropriate process detailed in Section 2.

- The system is a new application in GSA.
- The system resides on infrastructures that have a GSA ATO concurred by the CISO or a FedRAMP IaaS provisional ATO.

If a system does not meet the criteria or eligibility established in this guide one of the other A&A processes in CIO-IT Security-06-30 must be used.

## 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. This procedural guide provides GSA Federal employees and contractors with significant security responsibilities, as identified in GSA Order CIO 2100.1, “GSA Information Technology (IT) Security Policy,” and other IT personnel involved in performing A&A activities for systems, the specific processes to follow for accomplishing A&A activities for systems under their purview following the Lightweight Security Authorization Process.

## 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](mailto: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 guidance documents and templates below are referenced within the body of this guide and are available on the GSA IT Security [Procedural Guides](#) and [Forms and Aids](#) InSite pages.

**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-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)”

**Templates:**

- Lightweight Security Authorization System Security and Privacy Plan (SSPP)
- FIPS 199 Security Categorization
- Digital Identity Acceptance Statement (DIAS)
- Security Assessment Report (SAR)
- POA&M Template (also available from [ispcompliance@gsa.gov](mailto:ispcompliance@gsa.gov))
- Certification Memorandum
- 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 identify, along with the criteria listed earlier, if a system is eligible to use the lightweight authorization process 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 1.1](#). The security categorization process described under Task C-2 in [Section 2.3.2](#) is used to determine a system's FIPS 199 level to see if the systems security categorization is Low or Moderate.
- **Privacy Threshold Assessment (PTA)/Privacy Impact Assessment (PIA).** GSA's [Privacy Act Program website](#) 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 and to re-certify them annually.
- **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 Authorization

The 90-day Limited 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:

- The information system's architecture must be approved by the OCISO Security Engineering Division (ISE).
- FIPS 199 Security Categorization
- PTA/PIA
- DIAS
- Unauthenticated external vulnerability scanning
- Unauthenticated external web application scanning
- 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. These assessment

activities, combined with a Penetration Test Report providing the results, 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 2-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 and will form the basis for the 90-day Security Authorization Package:

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

The package with exception of the Penetration Test Report will be prepared by the supporting ISSO.

**Note:** A 90-day Limited ATO should not be extended, a system's ATO should be converted to one of the following ATOs or another ATO following one of the other A&A processes defined in CIO-IT Security-06-30.

- A FIPS 199 Low system can be issued a full three-year ATO after completion of the processes in Section 2.3 of this guide during the 90-day Limited ATO.
- A FIPS 199 Moderate system can be converted to a One-year Limited ATO after completion of the processes in Section 2.3 of this guide during the 90-day Limited ATO.

### **2.3 One-Year Limited ATO for FIPS 199 Moderate and Three-Year ATO for FIPS 199 Low Impact Systems**

Following the Lightweight security authorization process FIPS 199 Moderate systems may achieve a one-year limited ATO while a FIPS 199 Low impact information systems may achieve a three-year ATO. The key activities in the Lightweight Security Authorization Process and its implementation of the NIST RMF are detailed in the following sub-sections.

### 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 Service/Staff Offices (S/SO) 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. Archer governance, risk, and compliance (GRC) is the repository for GSA’s system inventory. Systems are registered in it as soon as they are identified and categorized as pending. They will stay in this status until they are placed into production. Systems following the process in this guide will be identified in Archer 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 GSA LATO 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), the sensitivity of the data the system handles, the user base, and the key points of contact. The system owner in collaboration with the ISSO completes these sections of the SSPP. These sections will also

**TASK C-2: Security Categorization** – Use GSA’s FIPS 199 Security Categorization Template to identify the information types handled by the system. Once completed it is summarized in the SSPP with the completed FIPS 199 template attached to the system’s SSPP. NIST SP 800-60 Volumes I and II are used to identify the information types handled by the system. The result of the system categorization is used in a future step to select security controls for the system. The data owner collaborates with the system owner and the ISSO to complete the template.

**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 and CISO or their designated representatives. The Chief Privacy Officer (CPO), or designated representative must approve the security categorization for systems with PII. 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 B](#). The Lightweight Security Authorization Process tailored baseline, as necessary, can be supplemented with additional controls and/or control enhancements 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 the AO in coordination with the ISSM and ISSO.

Document the selected security controls including any controls or enhancements selected above the baseline for the information system in the LATO SSPP template available on the [GSA 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 be aligned with the RMF Monitor Step and CIO-IT Security-12-66 and CIO-IT Security-21-114 (this guide is under development). The system-level strategy is to 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 LATO 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. When the LATO SSPP has been completed by the System Owner, ISSO (and Vendor ISSO if applicable), and the ISSM, it is signed by each party.

**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 OCISO ISE Division must review and approve the Security Architecture before the system's security controls are implemented. Additional details on developing and having the SSPP approved are contained in CIO-IT Security-21-114 (this guide is under development).

#### 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 LATO 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 DHS Cybersecurity Directives include specific implementation instructions which must be adhered to in order to secure the system and comply with the requirement.

The security control implementation descriptions should include planned inputs, expected behavior, and expected outputs (where appropriate) that are typical for technical controls. The SSPP should 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 LATO SSPP. This section must provide a thorough description of how the LATO security controls for the system are being implemented or planned to be implemented. Detailed instructions for completing the LATO SSPP are in the GSA LATO SSPP template, available on the [GSA IT Security Forms and Aids InSite page](#). For each control, descriptions must include:

- Describing how (including, what, when, where, and who) the security control is being implemented or planned to be implemented for all parts of the control;
- Identifying any scoping guidance that has been applied, including the type and;
- Explaining how all specified parameters have been met (i.e., not just stating they have been met, describe the how);
- Establishing time bound plans are described for planned controls;
- Ensuring controls identified as Not Applicable a rationale and supporting evidentiary artifacts must be provided.
- Systems with multiple components or subsystems must describe control implementations across all components.
- Systems leveraging a cloud solution must describe how the customer responsibilities in the CSP's CRM are implemented.

Systems leveraging a cloud solution must implement the customer responsibilities identified in the Cloud Service Provider's (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 LATO SSPP.

**Task I-2: Update Control Implementation** - During development, or in the course of operating and maintaining the system, the implementation details of controls may change. Changes occur for many reasons, including by not limited to infeasibility of the design, new capabilities being made available, patches and upgrades to the system. The LATO SSPP must be updated to reflect any changed implementation details so the LATO 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 LATO 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."

**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 B](#) identifies the security controls requiring assessment and the responsible assessor. The following sections further define 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, etc.), and manual review. For cloud environments such as AWS, the authenticated scan shall 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, etc.), 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.

#### *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 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.

**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 LATO SSPP (Control PL-2) can be consolidated into one finding and associated with PL-2. All other findings (including scan findings) rated Low or above are reported individually in the SAR.

Additional information on addressing findings based on the source of 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** - The ISSO collaborates with the System Owner, other system personnel, and the ISSM and prepares the POA&M as follows:

POA&Ms based on the vulnerabilities and recommendations included in the SAR:

- Do not include in the POA&M vulnerabilities identified as “Remediated” or “False Positive” in the SAR.
- Include in the POA&M all other vulnerabilities (including scan findings) in the SAR as individual POA&Ms.

The POA&M describes how the System Owner intends to address vulnerabilities (i.e., reduce, eliminate, or mitigate vulnerabilities). A POA&M Template and details on developing POA&Ms are contained in the POA&M procedural guide and on the POA&M Guidance Google Shared Drive. A GSA POA&M Template may be obtained by contacting [ispcompliance@gsa.gov](mailto:ispcompliance@gsa.gov).



Update the system's SSPP to reflect the results of the security assessment and any modifications to the security controls in the information system. This is necessary to account for any modifications made to address recommendations for corrective actions from the security assessor. Following completion of security assessment activities, the SSPP should reflect the actual state of the security controls implemented in the system. Update the GSA Control Tailoring Workbook and applicable Control Implementation Summary. The updated documents must be included as appendices to the system's SSPP.

**Note:** GSA tracks all POA&Ms on POA&M Shared Drives which serve as the primary tool for the management, storage, and dissemination of GSA POA&Ms.

### 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. For GSA's LATO process, the security authorization package includes:

- **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)
  - Appendix A – Acronyms
  - Attachments: Additional Supporting Documents (as necessary, see note below)

**Note:** Systems receiving a 1-year LATO or 3-year full ATO would have Attachments 4-5 of the SSPP as listed above typically included in the SAR instead of the SSPP.

- **CRM** – Please contact your ISSM to receive the vendor's current CRM for your system
- **POA&M**
- **Certification Memorandum**
- **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 in consultation with the CISO, System Owner, ISSM, ISSO, and others as necessary determines 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 prioritization of risks POA&Ms can be prioritized 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 of 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 detailed in CIO-IT Security-21-114—this guide is under development—and is summarized as follows:

- IST quality checks and validates the package and prepares a Certification Memorandum 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 corrective 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.”

**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, 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 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 or 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;

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: Lightweight Security Authorization ATO Package

Listed in the table below are the documents required for the Lightweight Security Authorization ATO Package. 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 A-1: Lightweight Security Authorization Process ATO Package**

Description
<b>SSPP</b> (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
<b>SAR</b> (with appendices/attachments) Appendix A - Acronyms Attachments: Additional Supporting Documents (as necessary, see note below)
<b>Note:</b> Systems receiving a 1-year LATO or 3-year full ATO would have Attachments 4-5 of the SSPP as listed above typically included in the SAR instead of the SSPP.
<b>CRM</b> - Please contact your ISSM to receive the vendor's current CRM for your system.
<b>POA&amp;M</b>
<b>Certification Memorandum</b>
<b>ATO Letter</b>

## Appendix B: Security 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 B. The ISSO Support Division (IST) has the responsibility for ensuring all of the security 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.

<b>L e g e n d</b>		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.
		Only required for systems following the One-Year Limited ATO for FIPS 199 Moderate and Three-Year ATO for FIPS 199 Low Impact Systems

800-53 Control	Control Title
AC-2	Account Management
AC-3	Access Enforcement
AC-6(5)	Least Privilege   Privileged Accounts
AC-6(9)	Least Privilege   Log Use of Privileged Functions
AU-2	Event Logging
AU-6(1)	Audit Record Review, Analysis, and Reporting   Automated Process Integration
CA-7	Continuous Monitoring
CA-8	Penetration Testing
CM-2(2)	Baseline Configuration   Automation Support for Accuracy and Currency
CM-3(1)	Configuration Change Control   Automated Documentation, Notification, and Prohibition of Changes
CM-6(1)	Configuration Settings   Automated Management, Application, and Verification
CM-7(5)	Least Functionality   Authorized Software - Allow-By-Exception
CM-8(2)	System Component Inventory   Automated Maintenance
CP-7(1)	Alternate Processing Site   Separation from Primary Site
IA-2	Identification and Authentication (Organizational Users)
IA-2 (1)	Identification and Authentication (Organizational Users)   Multifactor Authentication to Privileged Accounts
IA-2 (2)	Identification and Authentication (Organizational Users)   Multifactor Authentication to Non-Privileged Accounts
PL-2	System Security and Privacy Plans
PL-8	Security and Privacy Architectures
RA-5	Vulnerability Monitoring and Scanning
SA-11(1)	Developer Testing and Evaluation   Static Code Analysis
SA-22	Unsupported System Components

---

SC-7	Boundary Protection
SC-8(1)	Transmission Confidentiality and Integrity   Cryptographic Protection
SC-28 (1)	Protection of Information at Rest   Cryptographic Protection
SI-2	Flaw Remediation
SI-4	System Monitoring
SI-4(2)	System Monitoring   Automated Tools and Mechanisms for Real-Time Analysis
SI-4(4)	System Monitoring   Inbound and Outbound Communications Traffic
SI-4(5)	System Monitoring   System-Generated Alerts
SI-7	Software, Firmware, and Information Integrity
SI-10	Information Input Validation