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

Revision 6

April 25, 2018

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 – April 25, 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

Approval

IT Security Procedural Guide: Lightweight Security Authorization Process, CIO-IT Security-14-68, Revision 6 is hereby approved for distribution.

5/1/2018

X Kurt Garbars

Kurt D. Garbars
Chief Information Security Officer
Signed by: KURT GARBARS

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

Table of Contents

1 Introduction 1

1.1 Purpose 2
1.2 Scope 2
1.3 Policy 3
1.4 References 3

2 Lightweight Security Authorization Process 4

2.1 Sprint 90-Day Limited Authorization 4
2.2 Standard 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 Step 1 – Categorize Information System 6
2.3.2 RMF Step 2 – Select Security Controls 7
2.3.3 RMF Step 3 – Implement Key Security Controls and Cloud Service Provider Customer Responsibilities 8
2.3.4 RMF Step 4 – Assess Security Controls 8
2.3.5 RMF Step 5 – Authorize Information System 10
2.3.6 RMF Step 6 – Security Control Monitoring 12

Appendix A: Lightweight Security Authorization ATO Package 13

Appendix B: Security Controls for the Lightweight Security Authorization Process 14

Table 1-1: Lightweight ATO Process Table 1
Table 1-2: CSF Functions Mapped to NIST SP 800-37 RMF Steps 2

1 Introduction

The General Services Administration (GSA) Lightweight Security Authorization Process is specific to new GSA information systems pursuing an agile development methodology AND 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) provisional ATO. The process in this guide allows Federal Information Processing Standards (FIPS) Publication (PUB) 199, "*Standards for Security Categorization of Federal Information and Information Systems*" Low and Moderate impact systems to be granted 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 Sprint Limited ATO (FIPS 199 Low only)	A Sprint 90-day authorization is based on an enhanced scanning and assessment process (ESAP), including automated vulnerability and web application scanning, and manual verification testing. Approval for use required from the CISO.
90 day Standard Limited ATO (FIPS 199 Low or Moderate)	A Standard 90-day authorization is based on an external assessment including automated vulnerability and web application scanning as well as automated and manual penetration testing.
One year Limited ATO (FIPS 199 Moderate)	A one year authorization based on completing all tasks in the Lightweight Security Authorization Process.
Three-year Full ATO (FIPS 199 Low)	A three year authorization based on completing all tasks in the Lightweight Security Authorization Process.

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, "*Managing Enterprise Risk*," resulting in a new three-year 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 4, "*Security and Privacy Controls for Federal Information Systems and Organizations,"* described as tailoring in NIST SP 800-37, Revision 1, *"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*." This approach has been used to more closely align with GSA business requirements (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 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 National Institute of Standards and Technology (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. Further information on how the CSF relates to GSA's lightweight security authorization process is contained in Section 2. 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 Table 1-2, the second column lists the RMF Steps aligned with the CSF functions. Details on the implementation of the RMF in the Lightweight Security Authorization Process is provided in Section 2.2. 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
Identify (ID): Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	RMF Step 1: Categorize Information System RMF Step 2: Select Security Controls
Protect (PR): Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	RMF Step 2: Select Security Controls RMF Step 3: Implement Security Controls
Detect (DE): Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	RMF Step 2: Select Security Controls RMF Step 3: Implement Security Controls
Respond (RS): Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	RMF Step 4: Assess Security Controls RMF Step 5: Authorize Information Systems RMF Step 6: Monitor Security Controls
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.	RMF Step 4: Assess Security Controls RMF Step 5: Authorize Information Systems RMF Step 6: Monitor Security Controls

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.

- Is an application in GSA pursuing an agile development methodology.
- Resides on infrastructure with 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. 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 Policy

GSA Order CIO 2100.1, Chapter 3, Paragraph 2e states:

(4) *GSA CIO-IT Security-14-68, Lightweight Security Authorization Process, can be used to issue a Limited ATO (LATO) to a low or moderate impact system for an initial ninety (90) day period based on the results of assessments (e.g., penetration test) described in it. This process is restricted to systems pursuing an agile development methodology and residing on infrastructures that have a GSA ATO concurred by the GSA CISO or a FedRAMP ATO. Systems following this process can receive a one year LATO for FIPS 199 Moderate or a full three year ATO for FIPS 199 Low impact systems only if the Risk Management Framework (RMF) Tasks 1-5 described in GSA CIO-IT Security-14-68 are completed.*

1.4 References

Federal Regulations/Guidance:

- Executive Order 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 Cybersecurity Framework, *"Framework for Improving Critical Infrastructure Cybersecurity"*
- NIST SP 800-37, Revision 1, *"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"*
- NIST SP 800-53, Revision 4, *"Security and Privacy Controls for Federal Information Systems and Organizations"*
- NIST SP 800-53A, Revision 4, "*Assessing Security and Privacy Controls in Federal 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 System to Security Categories*"

GSA Guidance:

- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- CIO-IT Security-06-30, "*Managing Enterprise Risk*"
- 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 Strategy*"

2 Lightweight Security Authorization Process

The first step in any A&A process is to determine the FIPS 199 security categorization level of the information system. 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 in Section 2.2.1 should be followed to determine a system's FIPS 199 level. Once the FIPS 199 security categorization is determined the criteria in Section 1.1 and the elgibility requirement in Section 2.1 will determine the security authorization process in this guide to use. 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.

2.1 Sprint 90-Day Limited Authorization

In addition to the other criteria for using the Lightweight Security Authorization Process, eligibility to enter into the Sprint 90-day Limited Authorization process is determined on a case-by-case basis and must be approved by the CISO.

The Sprint 90-day Limited Authorization is available to systems at the FIPS 199 Low impact level. The Sprint 90-day Limited ATO is based upon conducting an ESAP, which includes automated vulnerability and web application scanning, and manual verification testing. The assessment will include the following activities:

- Unauthenticated external vulnerability scanning
- Unauthenticated external web application scanning
- External manual testing to verify identified vulnerabilities

External vulnerability and web application scanning will be conducted by the OCISO Security Operations (ISO) Division while manual verification testing will be conducted by the OCISO Information System Security Officer (ISSO) Support (IST) Division. These assessment activities, combined with a Penetration Test Report providing the results, will be completed within one (1) week of approval of the system's defined Rules of Engagement (RoE).

Any Very High/Critical or High vulnerabilities identified during assessment activities must be fixed or mitigated prior to Sprint 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 one week period, the test report will be issued "as is."

An ESAP Test Report, Plan of Action and Milestones (POA&M), and ATO letter will form the basis for the Sprint 90-day Security Authorization Package. The package with exception of the ESAP Test Report will be prepared by the supporting ISSO.

Note: A Sprint 90-day Limited ATO cannot be extended, the system's ATO can be converted to a full three year ATO after completion of the processes in Section 2.3 of this guide during the 90-day Limited ATO.

2.2 Standard 90-Day Limited Authorization

The Standard 90-day Limited Authorization process is available to systems at the FIPS 199 Low and Moderate levels. The Standard 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:

- 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 RoE.

Any Very High/Critical or High vulnerabilities identified during assessment activities must be fixed or mitigated prior to Standard 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."

A Penetration Test Report, POA&M, and ATO letter will form the basis for the Standard 90-day Security Authorization Package. The package with exception of the Penetration Test Report will be prepared by the supporting ISSO.

Note: A Standard 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 converted to 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

The Lightweight ATO process is applicable for FIPS 199 Low and Moderate systems. FIPS 199 Moderate systems may achieve a one-year limited ATO while 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 Step 1 – Categorize Information System

TASK 1-1: Security Categorization - Categorize the information system using the FIPS 199 Security Categorization Template and document the results of the security categorization in the System Security Plan/Security Assessment Report/Test Cases (SSP/SAR/Test Cases) document; use the template listed in Appendix A. The security categorization process is carried out by the Data Owner in cooperation and collaboration with appropriate organizational officials with information security/risk management responsibilities including but not limited to the Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), and the System Owner. The process for determining the appropriate impact level is outlined in FIPS 199 and its associated NIST publications: NIST SP 800-60 Volume I, Revision 1, Volume I, *"Guide for Mapping Types of Information and Information Systems to Security Categories"* and NIST SP 800-60 Volume II, Revision 1, Volume II, *"Appendices to Guide for Mapping Types of Information and Information System to Security Categories."* Please refer to the template and these documents to categorize the information system.

TASK 1-2: Information System Description - Describe the information system (including system boundary) and document the description in the SSP/SAR/Test Cases document. It provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. Descriptive information about the information system is documented in sections 1-11. The following sections should be sufficiently detailed:

- Section 1 identifies the system name and unique identifier.
- Section 2 provides the FIPS 199 categorization of the system. It must be supported by an FIPS 199 Security Categorization Template.
- Sections 3-8 identify roles/points of contact and system operational status and type.
- Section 9 describes the function or purpose of the system and its processes.
- Section 10 describes the technical system including an inventory of all hardware, software, and networking devices in the system's authorization boundary.
- Section 11 lists interconnections to other systems including details such as type of connection, security of the connection, and points of contact.

Note: Many interconnections require an Interconnection Security Agreement/Memorandum of Understanding/Memorandum of Agreement (ISA/MOU/MOA). Per GSA IT Security Policy 2100.1, "*Written management authorization for system interconnection, based upon the acceptance of risk to the IT system, must be*

obtained from the AOs of both systems prior to connecting a system not under a single AO's control IAW NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems. Per NIST SP 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc."

TASK 1-3: Information System Registration - Register the information system with the appropriate organizational program/management offices and the OCISO.

The ISSM shall coordinate with OCISO ISP to have the system added to the official GSA IT System Inventory repository.

2.3.2 RMF Step 2 – Select Security Controls

TASK 2-1: Security 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 SSP/SAR/Test Cases document using the template provided in Appendix A.

TASK 2-2: Monitoring Strategy - Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation. The key tasks involved in continuous monitoring are identified in CIO-IT Security-12-66, "*Information Security Continuous Monitoring Strategy*," and can be used as a guide for preparing the monitoring strategy.

TASK 2-3: Security Plan Approval - Review and approve the SSP/SAR/Test Cases document. The System Owner shall jointly develop the SSP/SAR/Test Cases document with the ISSO. The completed SSP/SAR/Test Cases document shall be submitted to the ISSM, IST Division Director, and to the ISE Division to determine if the plan is complete, consistent, and satisfies the security requirements for the information system. ISE will evaluate the security architecture and must approve it; the ISSM and Division Director must approve the SSP/SAR/Test Cases document.

Based on the results of the review, the SSP/SAR/Test Cases document may require further update or may be approved. Once approved, the SSP/SAR/Test Cases document establishes the set of security controls (system-specific, hybrid, and/or common controls) proposed to meet the security requirements for the information system; allowing Step 3 of the RMF to begin.

2.3.3 RMF Step 3 – Implement Key Security Controls and Cloud Service Provider Customer Responsibilities

TASK 3-1: Security Control Implementation – Implement the security controls selected in Task 2-1 and the Cloud Service Provider (CSP) Customer Responsibilities Matrix (CRM) available from the system's ISSM. The CRM identifies the control considerations that are customer responsibilities. The customer responsibilities are presented in checklist format and must be reviewed and their implementation verified by the Program Office/System Owner. The System Owner shall attest to implementation of the CSP determined customer responsibilities they are using.

Security tools shall be coordinated with the ISO division and as much as possible integrate with what is currently used at GSA or what GSA OCISO proposes to use, particularly in cloud environments. IT systems shall be configured and hardened using GSA IT security hardening guidelines, NIST guidelines, Center for Internet Security (CIS) guidelines, or industry best practice guidelines, as deemed appropriate by the AO and concurred by the OCISO. Implemented hardening checklists must be integrated with Security Content Automation Protocol (SCAP) content if available and/or to the greatest extent possible.

TASK 3-2: Security Control Documentation - Document security control implementation in section 13 of the SSP/SAR/Test Cases document. This section must provide a thorough description of how each of the required controls are implemented or planned to be implemented. The SSP/SAR/Test Cases document should 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 control assessment in RMF Step 4.

2.3.4 RMF Step 4 – Assess Security Controls

TASK 4-1: Security Control Assessment - Upon implementation of security controls in RMF Step 3, security control assessment will be performed by the IST Division to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements.

Assessment activities begin upon instantiation (i.e., build out) of the cloud environment and supported application, hardening consistent with GSA and system/environment control requirements, code freeze, a fully developed and approved SSP/SAR/Test Cases document, and provision of authentication information to the CSP's environment, virtual machines, and hosted application. The assessment activities will begin with a formal kick-off meeting including all stakeholders to review and finalize a project schedule.

An Integrated Project Team (IPT) approach inclusive of the team responsible for the infrastructure, application developers, system owner, OCISO, and other stakeholders (as necessary) is required to complete assessment activities in a timely fashion. The expected ATO timeline could be delayed without full commitment from all parties to fully develop the environment/application consistent with the minimum requirements identified in this guide,

provide requisite access to the environment, servers, and applications, and/or timely remediation of deficiencies identified during assessment.

Appendix B identifies the security controls requiring assessment and the responsible assessor. The sections below define each of the assessment types further.

Security Controls Assessment

The security controls assessment will be completed using the GSA SSP/SAR/Test Cases document identified in Appendix A. Controls assessments may include documentation review, manual validation/review using the CSP's portal (e.g., AWS Web Console), and technical controls assessment. Assessment will be performed on all of the security controls identified in Task 2-1.

CM-6 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 planned to be 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).

RA-5 Vulnerability Scanning / SI-2 Flaw Remediation

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 planned to be 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 agreement with CIO-IT Security-11-51.

TASK 4-2: Security Assessment Report (SAR) – The SSP/SAR/Test Cases document will document the issues, findings, and recommendations from the security control assessment. It will document assessment findings with recommendation(s) and risk determinations using the template listed in Appendix A. The report must individually identify and discuss findings from:

- Security control assessments;
- Vulnerability scans (all Critical/Very High, High, and Moderate vulnerabilities);
- Configuration scans (all non-compliant settings without approved deviations);
- Penetration test vulnerabilities.

TASK 4-3: Remedial Action - Conduct initial remediation actions on security controls based on the findings and recommendations and reassess remediated control(s), as appropriate. Findings that are remediated should be appropriately marked in the SSP/SAR/Test Cases document. In the SSP/SAR/Test Cases document, include “Mitigated” or “Resolved” next to the NIST SP 800-53 Control Heading.

2.3.5 RMF Step 5 – Authorize Information System

Following assessment of the information system in RMF Step 4, the POA&M is updated based on the results of the security assessment and any remedial action to correct findings; the Lightweight Security Authorization Process ATO Package (see Appendix A) is assembled and submitted to the AO for adjudication. 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 following tasks detail the actions in RMF Step 5.

TASK 5-1: Plan of Action and Milestones – The ISSO prepares the POA&M based on the findings and recommendations of the SSP/SAR/Test Cases document, excluding any remediation actions taken. The POA&M must include all vulnerabilities (except those identified as “Mitigated” “Resolved”) in the information system as documented in SSP/SAR/Test Cases document. The

POA&M describes how the System Owner intends to address those vulnerabilities (i.e., reduce, eliminate, or request acceptance of vulnerabilities). Use the POA&M template listed in Appendix A.

Update the SSP/SAR/Test Cases document to reflect the results of the security assessment and any modifications to the security controls in the information system. The SSP/SAR/Test Cases document should reflect the actual state of the security controls implemented in the system following completion of security assessment activities. This is necessary to account for any modifications made to address recommendations for corrective actions from the security assessor.

Note: For every Open or Outstanding finding in the SSP/SAR/Test Cases document there must be a related planned action in the POA&M and in the document for the NIST SP 800-53 control or enhancement.

TASK 5-2: Security Authorization Package – The ISSO assembles the Security Authorization Package and submits to the IST Division. It documents the results of the security assessment and includes the:

- SSP/SAR/Test Cases document
- Vulnerability Scan Data
- Penetration Test Report
- POA&M
- CRM
- ATO Letter

The IST Division will review the package and forward the ATO Letter to the CISO for concurrence if the package is completed consistent with the requirements in this guide and are free of Critical/Very High or High risk findings.

Upon CISO signature, the package can be submitted to the AO for ATO consideration. The security authorization package provides the AO the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

TASK 5-3: Risk Determination - Upon receipt of the final Lightweight Security Authorization Process ATO Package the AO must assess the information provided by the System Owner as documented in the ATO Package regarding the current security state of the system and the recommendations for addressing any residual risks.

TASK 5-4: Risk Acceptance – The AO shall determine, with advisement from the CISO, if the risk to GSA operations, assets, individuals, other organizations, or the Nation is acceptable. The explicit acceptance of risk is the responsibility of the AO. The AO must consider many factors, balancing security considerations with mission and operational needs. The AO issues an authorization decision for the information system after reviewing all of the relevant

information. Following review of the ATO package and consultation with the GSA CISO, the AO must render a decision to:

- Authorize system operation w/out any restrictions on its operation;
- Authorize system operation w/restriction(s) on its operation. The POA&M must include detailed corrective actions for deficiencies; or
- Not authorize the system for operation.

2.3.6 RMF Step 6 – Security Control Monitoring

After the system has been authorized for operation in RMF Step 5, its security controls must be monitored to determine if they continue to be implemented correctly, operated as intended, and producing the desired outcome to maintain an acceptable security posture. The following tasks detail the actions in RMF Step 6.

TASK 6-1: Information System and Environment Changes – The System Owner and ISSO will determine if changes to the system or its environment impact system security. Configuration and change management must be monitored, assessed, and approved after considering security impact.

TASK 6-2: Ongoing Security Control Assessments and Remediation Actions – The System Owner and ISSO will assess security controls and mitigate or remediate any findings from ongoing assessments as part of GSA's and the system's continuous monitoring processes.

TASK 6-3: Key Updates – The System Owner and ISSO will update the system's security documentation (SSP/SAR/Test Cases document, CRM, POA&M, vulnerability scan data, penetration test report, as applicable) based on changes or security assessments so the AO and CISO can be kept informed of the system's state and security posture.

TASK 6-4: Ongoing Risk Determination and Acceptance – The AO will determine, with advisement from the CISO, if the ongoing risk to GSA operations, assets, individuals, other organizations, and the Nation continues to be acceptable, after considering changes to the system, its environment, and the results from ongoing assessments. Based on this determination, the AO in consultation with the CISO, will determine if reassessment and reauthorization is required earlier than the system's ATO would indicate.

Appendix A: Lightweight Security Authorization ATO Package

Listed in the table below are the documents required for the Lightweight Security Authorization ATO Package. Where available, links are provided to the GSA InSite webpage, Google Drive, or Google document where the ATO Package templates are located.

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

Lightweight Security Authorization Process ATO Package
Documents
System Security Plan/Security Assessment Report/Test Cases (SSP/SAR/Test Cases): SSP/SAR/Test Cases Template
Vulnerability Scan Data
Penetration Test Report Template
POA&M Template Google Sheet
Customer Responsibility Matrix (CRM): Please contact your Information System Security Manager (ISSM) to receive the vendor's current CRM for your system.
ATO Letter

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 combined SSP/SAR/Test Cases template identified in Appendix A. 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.

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-2	Account Management
AC-3	Access Enforcement
AC-6(5)	Least Privilege | Privileged Accounts
AC-6(9)	Least Privilege | Auditing Use of Privileged Functions
AU-2	Audit Events
AU-6(1)	Audit Review, Analysis, and Reporting | Process Integration
CA-8	Penetration Testing
CM-2(2)	Baseline Configuration | Automation Support for Accuracy / Currency
CM-3(1)	Configuration Change Control | Automated Document / Notification / Prohibition of Changes
CM-6(1)	Configuration Settings | Automated Central Management / Application / Verification
CM-7(5)	Least Functionality | Authorized Software / Whitelisting
CM-8(2)	Information System Component Inventory | Automated Maintenance
CP-7(1)	Alternate Processing Site | Separation From Primary Site *(only when availability is a concern)*
IA-2	Identification and Authentication (Organizational Users)
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts
PL-8	Information Security Architecture
RA-5	Vulnerability Scanning
SA-11(1)	Developer Security Testing and Evaluation | Static Code Analysis
SA-22	Unsupported System Components
SC-7	Boundary Protection
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection
SC-28 (1)	Protection of Information At Rest | Cryptographic Protection
SI-2	Flaw Remediation
SI-4	Information System Monitoring
SI-4(2)	Information System Monitoring | Automated Tools for Real-Time Analysis
SI-4(4)	Information System Monitoring |Inbound and Outbound Communications Traffic
SI-4(5)	Information System Monitoring | System-Generated Alerts
SI-7	Software, Firmware and Information Integrity
SI-10	Information Input Validation