IT Security Procedural Guide: Moderate Impact Software as a Service (MiSaaS) Authorization Process CIO-IT Security-18-88

Revision 2

March 19, 2025

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – June 6, 2018		
1	Dean/ Klemens	Initial Draft	N/A	N/A
		Revision 1 - March 31, 2022		
1	Dean	Revisions include: ● Updated to NIST SP 800-37, Revision 2 process. ● Updated to NIST SP 800-53, Revision 5 security and privacy controls.	Update to the latest Federal, NIST, and GSA guidance	Throughout
		Revision 2 - March 19, 2025		
1	Normand/ Klemens/ Peralta	Revisions include: ● Added requirement for CISO and AO approval to use the MiSaaS process. ● Added system assessment required by a certified A2LA 3PAO. ● Added SI-02(03) and updated privacy controls in baseline. ● Replaced Table 2-1 with Table from Appendix and removed duplicative table in Appendix. ● Added sections on ATO Extensions and Failure to Meet/Maintain ATO Requirements. ● Added leading zeros to controls and updated to current guide format and style.	Update to align with GSA guidance.	Throughout

Approval

IT Security Procedural Guide: Moderate Impact Software as a Service (MiSaaS) Security Authorization Process, CIO-IT Security-18-88, Revision 2 is hereby approved for distribution.

Signed by:
Dovarius Peoples
34793F3A1E88420...

Dovarius Peoples
Acting GSA Chief Information Security Officer

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

Table of Contents

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.

1 Introduction

The General Services Administration (GSA) Moderate Impact Software as a Service (MiSaaS) Security Authorization Process is specific to new GSA information systems pursuing an agile development methodology and residing on infrastructures that has, or is in the process of obtaining, a Federal Risk and Authorization Management Program (FedRAMP) provisional authorization to operate (ATO). The process in this guide allows for a Federal Information Processing Standard (FIPS) Publication (PUB) 199, "Standards for Security Categorization of Federal Information and Information Systems" FIPS 199 Moderate impact system to be granted a one year ATO after completing the tailored National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, "Revision 2, Risk Management Framework (RMF) for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy" processes detailed in this guide. **Prior to a system using the MiSaaS Process, the GSA Chief Information Security Officer (CISO) and Authorizing Official (AO) must approve its usage by email to the IST and ISP Directors and the Chief Privacy Officer (CPO).**

Conditions for using the MiSaaS authorization process:

- Must be built on infrastructure that has or is in the process of obtaining a FedRAMP authorization to operate (ATO);
- The vendor is able and willing to document and assess all applicable security requirements at their cost;
- The system assessment must be conducted by an American Association for Laboratory Accreditation (A2LA) Certified Third Party Assessment Organization (3PAO).

The MiSaaS 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. 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 or are pursuing 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) 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. For more information on GSA's alignment of the RMF to the CSF, refer to CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk.

In support of EO 13800, GSA has aligned its risk management processes with the CSF. The five core CSF Functions are listed in Table 1-1, the second column lists the RMF Steps aligned with the CSF functions in the MiSaaS process. Details on the implementation of the RMF in the MiSaaS Process is provided in Section 2.

Note: GSA is in the process of developing and updating GSA Order CIO 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 1-1. 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 (ID.GV) **Categorize** Task C-1, System Description (Profile) Task C-2, Security Categorization (ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5, Profile) Task C-3, Security Categorization Review and Approval (N/A) **Select** Task S-1: Control Selection (Profile) Task S-5: Continuous Monitoring Strategy – System (ID.GV, DE.CM) **Assess** Task A-6: Plan of Action and Milestones (ID.RA-6) **Authorize** Task R-3: Risk Response (ID.RA-6) **Monitor** Task M-1: System and Environment Changes (DE.CM, ID.GV) Task M-2: Ongoing Assessments(ID.SC-4)
Protect (PR): Develop and implement appropriate safeguards to ensure delivery of critical services.	**Select** Task S-1: Control Selection (Profile) **Implement** Task I-1: Control Implementation (PR.IP-1, PR.IP-2) Task I-2: Update Control Implementation Information (PR.IP-1, Profile)
Detect (DE): Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	**Select** Task S-1: Control Selection (Profile) Task S-5: Continuous Monitoring Strategy – System (DE.CM, ID.GV) **Monitor** Task M-1: System and Environment Changes (DE.CM, ID.GV)
Respond (RS): Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.	**Select** Task S-1: Control Selection (Profile) **Monitor** Task M-4: Authorization Package Updates (RS.IM)
Recover (RC): Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	**Select** Task S-1: Control Selection (Profile)
No CSF Function Mapping	**Select** Task S-6: Plan Review and Approval (N/A) **Assess** Task A-3: Control Assessments (N/A) Task A-4: Assessment Reports (N/A) Task A-5: Remediation Actions (Profile) **Authorize** Task R-1: Authorization Package (N/A) Task R-2: Risk Analysis and Determination (N/A) Task R-4: Authorization Decision (N/A)

1.1 Purpose

This procedural guide defines a security authorization process for FIPS 199 Moderate Impact SaaS systems to be granted a one year ATO upon successfully completing the processes detailed in Section 2.

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 CIO 2100.1 and other IT personnel involved in performing assessment and authorization (A&A) activities for systems, the specific processes to follow for accomplishing A&A activities for systems under their purview following the MiSaaS Security Authorization Process.

1.3 References

Federal Regulations/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

GSA Policies, Procedures, Guidance:

- GSA Order CIO 2100.1, GSA Information Technology (IT) Security Policy

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page with the exception of CIO-IT Security-09-44 which is restricted. It is available on the internal GSA InSite IT Security Procedural Guides page.

- CIO-IT Security-01-05: Configuration Management (CM)

- CIO-IT Security-04-26: Federal Information Security Modernization Act (FISMA) Implementation
- CIO-IT Security-06-30: Managing Enterprise Cybersecurity 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 (ISCM) Strategy & Ongoing Authorization (OA) Program
- CIO-IT Security-18-91: Risk Management Strategy (RMS)

2 Moderate Impact SaaS Security Authorization Process

The key activities in the MiSaaS authorization process and its implementation of the NIST RMF are detailed in the following sub-sections.

- RMF Prepare Step
- RMF Categorize Step
- RMF Select Step
- RMF Implement Step
- RMF Assess Step
- RMF Authorize Step
- RMF Monitor Step

The MiSaaS security authorization process is a tailored version of the NIST RMF. The MiSaaS RMF steps do not include all of the tasks in the NIST RMF steps. The MiSaaS process typically takes 2-5 months to complete. The time to complete the process is dependent on the readiness of the system at the start of the process (i.e., have all of the security controls been implemented) and responsiveness (i.e., how quickly responses for additional information are provided) throughout the process.

2.1 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 Information System Security Officers (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 will stay in this status until they are placed into production.

2.2 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 MiSaaS System Security and Privacy Plan (SSPP) template. The System Owner in collaboration with the ISSO completes these sections of the SSPP. These 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.

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 MiSaaS 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 Authorizing Official (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 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 MiSaaS Security Authorization Process are identified in Appendix A. The MiSaaS 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 MiSaaS SSPP document.

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 RMF Step Monitor and CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program. The strategy is to address monitoring of controls that are not monitored as part of GSA's ISCM strategy and the frequency of monitoring. It defines how system changes are monitored, how risk assessed, and reporting on monitoring and the reporting of results. The System Owner collaborates with the ISSM, ISSO, Privacy Team as necessary, and others to establish the system-level continuous monitoring strategy.

Task S-6: Plan Review and Approval – The MiSaaS SSPP must be reviewed and approved. The System Owner collaborates with the ISSM, ISSO, Data Owners, Privacy Team as necessary, and other System Owners (regarding common/hybrid controls), and others to complete the MiSaaS 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 MiSaaS SSPP has been completed by the System Owner, ISSO (and Vendor ISSO if applicable), and the ISSM it is signed by each of them.

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).

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

2.4 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 in the MiSaaS 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.

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.

Systems 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 MiSaaS control set (see Appendix A) must be addressed.

Federal requirements such as DHS Cybersecurity Directives include specific implementation instructions which must be adhered 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 control assessment in Task S-1.

Security controls are documented in Section 13 of the MiSaaS SSPP. This section must provide a thorough description of how the MiSaaS security controls for the system are being implemented or planned to be implemented. Detailed instructions for completing the MiSaaS SSPP are in the GSA MiSaaS SSPP Template, on the InSite IT Security Forms and Aids webpage. 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 how they are met);
- 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.

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 MiSaaS 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 MiSaaS SSPP must be updated to reflect any changed implementation details so the MiSaaS SSPP always reflects the "as implemented" state of the system. In this manner when assessments occur–the next RMF step–the assessors can determine if the system reflects its documented state or if 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 MiSaaS SSPP as necessary.

2.5 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 - The system assessment must be conducted by an A2LA certified 3PAO. Assessors assess the security controls following the Security Assessment Plan (SAP) and using the MiSaaS Test Cases, including any supplemental or updated tests based on the specific system as identified in the SAP (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.

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 SSPP, 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 A identifies the security controls requiring assessment and the responsible assessor. The sections below define each of the assessment types further.

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).

Vulnerability Monitoring and Scanning/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: Conducting Penetration Test Exercises.

TASK A-4: Assessment Reports – Assessors prepare a Security Assessment Report (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, "Guide for Conducting Risk Assessments." Multiple findings regarding the MiSaaS SSPP (Control PL-02) can be consolidated into one finding and associated with PL-02. 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 InSite. 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 on the InSite Forms and Aids page. 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 Plan of Action and Milestones (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 identified risks. Details on developing POA&Ms are contained in 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 page. POA&M assistance is available by contacting ispcompliance@gsa.gov.

Update the MiSaaS 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 (CTW) and applicable Control Implementation Summary Table. The updated documents must be included as appendices to the MiSaaS 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 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.

2.6 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.”

Note: A MiSaaS ATO is a commitment to sponsor a CSP for a FedRAMP Moderate ATO if the vendor is not being sponsored by another agency.

TASK R-1: Authorization Package – The ISSO assembles the security authorization package. Listed in Table 2-1 are the documents required for a MiSaaS ATO Package.

Table 2-1. MiSaaS Security Authorization Process ATO Package

Moderate Impact Software as a Service (MiSaaS) Security Authorization Process
Documents
System Security and Privacy Plan (with appendices/attachments) Appendix A - References Attachment 1: Privacy Threshold Analysis/Privacy Impact Assessment Attachment 2: FIPS 199 Security Categorization Attachment 3: Digital Identity Acceptance Statement Attachment 4: Information exchange agreement/Interconnection security agreement/Memorandum of agreement (IEA/ISA/MOA) (if applicable) Attachment 5: Control Tailoring Workbook (CTW) Attachment 6: Control Implementation Summary Table (for MiSaaS) Attachment 7: Contingency Plan (with Business Impact Analysis) Attachment 8: Contingency Plan Test Report Attachment 9: Incident Response Plan Attachment 10: Continuous Monitoring Plan Attachment 11: Code Review Report (if applicable)
Security Assessment Report (Results from the Security Assessment Plan) Appendix A - Acronyms Attachment 1: Security Assessment Plan (SAP) Attachment 2: GSA NIST SP 800-53, Revision 5 Test Case Workbook Attachment 3: Authenticated OS Vulnerability Scan Results Attachment 4: Authenticated Web Application Vulnerability Scan Results Attachment 5: Penetration Test Report (if applicable) Attachment 6: Other Scan Reports, as necessary
POA&M
CRM - Please contact your ISSM to receive the vendor's current CRM for your system.
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 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 summarized as follows:

- IST quality checks and validates the package and prepares a Certification Memorandum and uploads documents to GSA's GRC tool (if not already uploaded).
- The ISSM prepares the ATO Letter and uploads it to DocuSign.
- For systems that have a PIA, the SAOP reviews and signs the letter (or directs changes).
- The CISO reviews the package and coordinates with the ISSM and others and signs the letter (or directs changes).
- The AO is briefed and based 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.

2.7 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: 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. The RMS states:

- IT changes are to be requested through a defined CM approval process (e.g., a chartered Configuration Control Board [CCB]) that documents the nature of the change, the criticality, impacts on the user community, testing and rollback procedures, stakeholders, and points of contact.

- System changes are to be tested and validated prior to implementation into the production environment.
- Configuration settings and configuration baselines are to be updated as necessary to meet new technical and/or security requirements and are controlled through the CM process.

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: Federal Information Security Modernization Act (FISMA) Implementation, GSA's annual 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.

- MiSaaS SSPP (and all appendices and attachments);
- POA&M.

Processes that may require updates to documents and POA&Ms include:

- 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 MiSaaS SSPP will be updated to reflect any changes

2.8 MiSaaS ATO Extensions

Extensions to MiSaaS ATOs will only be granted in special circumstances and must be approved by the GSA CISO and the corresponding AO. Extensions may be granted under the following circumstances:

- The vendor needs additional time to complete its FedRAMP ATO and/or for GSA to transition to a Leveraged FedRAMP ATO; or
- GSA needs time to transition from a current MiSaaS solution to another solution.

2.9 Failure to Meet/Maintain MiSaaS ATO Requirements

If at any time, the vendor is either unwilling or unable to meet any of the requirements specified in this guide, the ATO shall be terminated upon approval of the AO. It is the responsibility of the assigned ISSO and GSA System Owner to ensure the requirements continue to be met. Significant changes regarding the MiSaaS solution shall be reported to the ISSM, who with the ISSO, manages the ATO package.

Appendix A. Security Controls for the MiSaaS Security Authorization Process

A security control assessment must be completed for each control in the table below. The 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.

Note: Manual inspection in AWS is to be performed via the AWS Console.

Table A-1. Legend for Table A-2

	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.

Table A-2. MiSaaS Security Controls

800-53 Control	Control Title
AC-02	Account Management
AC-02(07)	Account Management | Privileged User Accounts
AC-03	Access Enforcement
AC-03(14)	Access Enforcement | Individual Access
AC-05	Separation of Duties
AC-06	Least Privilege
AC-06(02)	Least Privilege | Non-Privileged Access for Non-Security Functions
AC-06(09)	Least Privilege | Log Use of Privileged Functions
AC-08	System Use Notification
AC-12	Session Termination
AC-21	Information Sharing
AT-03(05)	Role-based Training | Processing Personally Identifiable Information
AU-02	Event Logging
AU-03	Content of Audit Records
AU-03(03)	Content of Audit Records | Limit Personally Identifiable Information Elements
AU-06	Audit Record Review, Analysis, and Reporting
AU-06(01)	Audit Record Review, Analysis, and Reporting | Automated Process Integration
AU-11	Audit Record Retention
CA-02	Control Assessments
CA-07	Continuous Monitoring
CA-08	Penetration Testing
CA-08(01)	Penetration Testing | Independent Penetration Testing Agent or Team
CM-02	Baseline Configuration
CM-02(02)	Baseline Configuration | Automation Support for Accuracy and Currency
CM-03	Configuration Change Control

800-53 Control	Control Title
CM-06	Configuration Settings
CM-06(01)	Configuration Settings | Automated Management, Application, and Verification
CM-07(02)	Least Functionality | Prevent Program Execution
CM-08	System Component Inventory
CP-02	Contingency Plan
CP-04	Contingency Plan Testing
CP-07	Alternate Processing Site
CP-09	System Backup
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
IA-02(12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials
IA-05	Authenticator Management
IA-05(07)	Authenticator Management | No Embedded Unencrypted Static Authenticators
IR-02(03)	Incident Response Training | Breach
IR-06	Incident Reporting
IR-08	Incident Response Plan
IR-08(01)	Incident Response Plan | Breaches
MP-06	Media Protection
PL-02	System Security and Privacy Plans
PL-08	Security and Privacy Architectures
PS-03	Personnel Screening
PS-07	External Personnel Security
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-02	Security Categorization
RA-03	Risk Assessment
RA-05	Vulnerability Monitoring and Scanning

800-53 Control	Control Title
RA-05(05)	Vulnerability Monitoring and Scanning | Privileged Access
RA-08	Privacy Impact Assessments
SA-08(33)	Security and Privacy Engineering Principles | Minimization
SA-09	External System Services
SA-10	Developer Configuration Management
SA-11(01)	Developer Testing and Evaluation | Static Code Analysis
SA-22	Unsupported System Components
SC-07	Boundary Protection
SC-07(04)	Boundary Protection | Personally Identifiable Information
SC-07(05)	Boundary Protection | Deny By Default — Allow By Exception
SC-07(08)	Boundary Protection | Route Traffic to Authenticated Proxy Servers
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection
SC-12	Cryptographic Key Establishment and Management
SC-13	Cryptographic Protection
SC-28(1)	Protection of Information At Rest | Cryptographic Protection
SI-02	Flaw Remediation
SI-02(03)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions
SI-03	Malicious Code Protection
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(16)	System Monitoring | Correlate Monitoring Information
SI-04(23)	System Monitoring | Host-Based Devices
SI-05	Security Alerts, Advisories, and Directives
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
SR-06	Supplier Assessments and Reviews
SR-08	Notification Agreements