# IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk
# CIO-IT Security-06-30

**Revision 26**

June 30, 2026

Office of the Chief Information Security Officer

# VERSION HISTORY/CHANGE RECORD*

*The version history/change record is limited to the last 3 versions of this guide. For information on previous versions contact ispcompliance@gsa.gov.

| Change Number | Person Posting Change | Change | Reason for Change | Page Number of Change |
|---|---|---|---|---|
| | | **Revision 24 – June 26, 2023** | | |
| 1 | Desai/Klemens/ McCormick/ Hanna | Revisions include:<br>● Updated CISA KEV POA&M and AOR information.<br>● Updated Table E-1, Showstopper Items/Controls.<br>● Revised Section 4.8: GSA Leveraged FedRAMP SaaS Solution Process<br>● Updated control implementation guidance, as necessary.<br>● Aligned to other guides.<br>● Updated to current format and structure.<br>● Updated system interconnection sections.<br>● Removed references to Clean ATO guide (not published) and processes based on it. | Updated to align with current GSA guidance. | Throughout |
| 2 | Privacy Office – Riordan, Hanna, Speidel | ● Updated the Senior Agency Official for Privacy's responsibilities and the Privacy office's engagement in the A&A process.<br>● Added the Chief Privacy Officer as a signatory of the guide. | Updated to align with current GSA guidance. | Throughout |
| | | **Revision 25 – October 16, 2024** | | |
| 1 | Normand/ Klemens/ Salamon | ● Updated guidance on SARs, POA&Ms, and AORs.<br>● Updated guidance on policy deviation approvals.<br>● Updated guidance on alignment to NIST SP 800-53, Revision 5.<br>● Updated Privacy team responsibilities based on GSA guidance.<br>● Updated information related to the Lightweight Security Authorization, Leveraged FedRAMP SaaS Solution, and GSA Pages (formerly Federalist) processes. | Updated to align with current GSA guidance. | Throughout |

| Change Number | Person Posting Change | Change | Reason for Change | Page Number of Change |
|---|---|---|---|---|
| | | ● Added information on Mobile Application Approval Process.<br>● Updated MOA, IEA, ISA information to align with CIO-IT Security-24-125: Managing Information Exchanges.<br>● Added section on assessing BMC solutions.<br>● Updated to include OMB M-22-18/M-23-16 and the IoT Act.<br>● Added CA-08(02), Red Team Exercises, and updated CA-03, Information Exchange information. | | |
| | | **Revision 26 – June 30, 2026** | | |
| 1 | Normand/ Salamon/ Klemens/ Peralta | ● Modified Moderate Leveraged FedRAMP SaaS assessment process.<br>● Changed Red Team Exercise requirement to be only for HVAs.<br>● Restructured Appendices to:<br>○ Appendix A: update references and links,<br>○ Appendix B: update data at rest encryption guidance,<br>○ Appendix C: Align to CSF 2.0,<br>○ Appendix D: Update A&A Process Package Document Lists,<br>○ Appendix E: Added significant change decision tree, and<br>○ Deleted an Appendix not referenced in the guide.<br>● Added a link to the GSA RMF RACI chart in the responsibilities section.<br>● Updated policy deviation requirement to include a Memorandum for Record, as necessary.<br>● Removed information on migrating to NIST SP 800-53, Revision 5.<br>● Updated to require HVAs to use the HVA control overlay for their authorization. | Updated to align with current GSA guidance. | Throughout |

| Change Number | Person Posting Change | Change | Reason for Change | Page Number of Change |
|---|---|---|---|---|
| | | ● Updated POA&M guidance on when a POA&M is required.<br>● Removed requirement for system level continuous monitoring plans. Systems must align to GSA's continuous monitoring processes.<br>● Removed references to rescinded OMB memos M-22-18 and M-23-16.<br>● Updated guidance on control tailoring regarding parameter assignments.<br>● Added guidance on authorization package updates based on GSA guidance changes.<br>● Removed table 5-1: Information Exchange Agreements.<br>● Changed showstopper controls to critical controls.<br>● Updated terminology from SSPP to SSP throughout the document. | | |

# Approval

IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk, CIO-IT Security-06-30, Revision 26, is hereby approved for distribution.

DocuSigned by:
Joseph Hoyt
CA8EF810EDA7425...

Joseph Hoyt
Acting GSA Chief Information Security Officer

**Contact: GSA Office of the Chief Information Security Officer (OCISO), Security Risk & Compliance Division (ISA) at ispcompliance@gsa.gov.**

# Concurrence

The undersigned concurs with the Privacy Officer's responsibilities established in this guide regarding the categorization, assessment, and authorization of GSA systems.

DocuSigned by:
Richard Speidel
171D5411183F40A...

Richard Speidel
GSA Chief Privacy Officer

**Contact: GSA Office of the Chief Privacy Officer (CPO) at privacy.office@gsa.gov.**

# Table of Contents

# Tables and Figures



Notes: Hyperlinks in this guide are provided as follows:

- Appendix A - Consolidated List of Guidance, Policies, Procedures, Templates. This appendix contains hyperlinks to Federal Regulations/Guidance and to GSA web pages containing GSA policies, guides, and forms/templates.
- In running text - Hyperlinks 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 document listed in Appendix A. For example, Google Forms, Google Docs, and websites will have links.

# 1 Introduction

The General Services Administration (GSA) uses two approaches to permit information systems, applications, services, features, or functions to be used.

- Authorization to Operate (ATO) - An official management decision authorizing the operation of a system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.
- Approval to Use (ATU) – A risk-based approval process for usage of services, features, or functions on information systems or platforms with an existing ATO.

Security Assessment and Authorization (A&A) processes within the GSA lead to an ATO and are based on the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and the security authorization process as described in NIST Special Publication (SP) 800-37, Revision 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.” This guide describes key activities in managing enterprise-level cybersecurity risk through a system life cycle perspective including information system ATO and continuous monitoring. Every GSA Information Technology (IT) system/platform must use one of the A&A processes identified in this guide or a pilot A&A process as described later in this section.

In Appendix B, Table B-1, GSA has identified a list of Critical items and NIST SP 800-53 Revision 5, “Security and Privacy Controls for Information Systems and Organizations,” controls associated with them, including compliance with Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directives (BODs) and Emergency Directives (EDs). The Critical items and controls associated with them, if not fully compliant, will keep a system from receiving a full ATO.

GSA may conduct pilots of additional A&A processes when a system or the evolving IT and IT security environments indicate a process different from any of GSA’s existing processes is preferred. Piloting of new processes must be coordinated with the GSA Chief Information Security Officer (CISO). Final approval of the process is indicated by the CISO concurring with any ATO resulting from the pilot.

ATU processes and procedures are based on evaluating the risk of using available services, features, or functions based on their characteristics and environment. Section 3 provides additional information on GSA’s ATU processes.

Any deviations from the security requirements established in GSA Order CIO 2100.1, “GSA Information Technology (IT) Security Policy” must be coordinated by the Information System Security Officer (ISSO) through the appropriate Information System Security Manager (ISSM) and approved by the Authorizing Official (AO) and CISO. Policy deviations must be documented using the GSA Memorandum for Record (MFR) - Policy Deviation template.

**NOTE:** MFRs are typically for an external (e.g., contractor) system implementing a control or security feature not aligned to GSA’s policy. For example, a contractor system may have a password policy that differs from GSA’s policy due to their internal policies or in support of other customers. Technology defects (i.e., a technology is unable to implement a GSA policy

requirement) should be documented in the system's System Security Plan (SSP), but do not require an MFR.

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." The National Institute of Standards and Technology (NIST) has published The NIST Cybersecurity Framework 2.0 (CSF 2.0) as the latest version of the Framework. 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 use of the NIST RMF is provided in Section 5 and Appendix C where the CSF categories and subcategories are defined and mapped to NIST SP 800-53 controls.

## 1.1 Purpose

This procedural guide defines the GSA cybersecurity risk management process. It addresses the security authorization processes GSA has implemented for information systems to obtain an ATO. This guide identifies ATU processes for services, features, and functions to be used at GSA, and the process for protecting Confidential Unclassified Information (CUI) in nonfederal systems. The guide describes the key activities in managing enterprise-level cybersecurity risk as described in NIST SP 800-37. This guide assists agency and contractor personnel to understand and fulfill their security responsibilities regarding ATO, ATU, and other processes.

## 1.2 Scope

The requirements outlined within this guide apply to all GSA Federal employees, contractors, and vendors who oversee/protect GSA information systems and data. The guide provides GSA Federal employees, contractors, and vendors as identified in CIO 2100.1 and other IT personnel involved in performing A&A activities with the specific processes to follow for properly accomplishing cybersecurity activities. All GSA systems must adhere to one of the processes described in this guide, the security requirements specified in CIO 2100.1, and the guides listed on the IT Security Technical Guides and Standards and IT Security Procedural Guides web pages. The following definitions are provided for classifying information systems/platforms within the scope of this guide.

- **Federal System (i.e., Agency System).** An information system in GSA's inventory processing or containing GSA or Federal information where the infrastructure and/or applications are NOT wholly operated, administered, managed, and maintained by a Contractor.
- **Contractor System.** An information system in GSA's inventory processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a contractor in non-GSA facilities.

## 1.3 Policy

As detailed within CIO 2100.1, Authorizing Officials (AOs) must ensure risk assessments are performed as part of A&A activities before a system is placed into production, when significant changes are made to the system, and as specified in this guide and the guides for GSA's other A&A processes.

## 1.4 GSA GRC Tool Implementation

The GSA has implemented its official agency system inventory in a Governance, Risk, and Compliance (GRC) tool. A read-only version of GSA's FISMA system inventory is available via the GSA EA Analytics & Reporting (GEAR) FISMA web page. As GSA continues implementing its A&A processes into its GRC tool, specific activities described in this guide will be incorporated in the GRC tool to take advantage of its automation capabilities. Any questions regarding the use of GSA's GRC tool should be sent to archersupport@gsa.gov.

### 1.4.1 Agency System Inventory

The agency system inventory in the GRC tool contains attributes such as responsible organization, system name, Federal Information Processing Standards Publication (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems" security categorization level, ATO type, and ATO date. The inventory includes an A&A repository for storing all system A&A documents and artifacts for GSA's systems.

### 1.4.2 Authorization Packages

Authorization packages have been created in GSA's GRC tool for GSA's systems and the task of implementing the authorization process for systems is just starting. The first steps in this process include inputting security categorization, privacy, and system demographics (boundary, connections, etc.) into the GRC tool, and allocating NIST SP 800-53 security controls. The GSA is conducting assessments in the GRC tool, and plans on implementing plans of action and milestones (POA&Ms) and the entire A&A process in the GRC tool.

## 1.5 Assessment and Authorization Roles and Responsibilities

There are many roles associated with the security authorization process. System Owners for each information system are responsible for ensuring their respective Service and Staff Office's (SSO) systems have been through the GSA A&A process, have received an ATO from the AO, and received concurrence from the GSA Office of the CISO (OCISO). The complete roles and responsibilities for agency management officials and others with significant IT Security responsibilities are defined fully in Section 4 of CIO 2100.1's GSA Cybersecurity Handbook. The following sections provide a high-level description of the responsibility for the primary roles with management and operational A&A responsibilities.

The RMF RACI Google Sheet contains a Responsible, Accountable, Consulted, and Informed (RACI) chart where GSA has associated RMF activities with GSA roles. The chart provides a granular view of who does what with regard to the RMF activities listed in the chart.

### 1.5.1 GSA Administrator

The GSA Administrator is responsible for ensuring an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of GSA.

### 1.5.2 Risk Executive (Function)

The Risk Executive (Function) at GSA is handled by the Enterprise Management Board (EMB), chaired by the Deputy Administrator who is also the Senior Accountable Official for Risk

Management (SAORM). For cybersecurity risks, the Enterprise Risk and Strategic Initiatives (ERSI) board, co-chaired by the Deputy Performance Improvement Officer and the CISO, identifies and monitors agency-wide risks and ensures the EMB is updated on the risks and impacts to GSA. The CISO, Authorizing Officials, and subject matter experts facilitate the consistent application of cybersecurity risk management across GSA.

### 1.5.3 GSA Chief Information Officer (CIO)

The GSA Chief Information Officer (CIO) has overall responsibility for the GSA IT Security Program. The CIO is responsible for providing guidance, assistance, support, and management processes to GSA staff and organizations to enable them to perform their responsibilities with regard to GSA's IT Security Program.

### 1.5.4 Chief Information Security Officer (CISO)

Public Law 113-283, "Federal Information Security Modernization Act of 2014" (FISMA), establishes the designation of a senior agency information security officer responsible for complying with Federal security requirements. GSA has assigned this role to the CISO. The CISO is the focal point for all GSA IT security and must ensure the security requirements described in this Order are implemented agency wide. The CISO reports directly to the CIO as required by FISMA.

### 1.5.5 GSA Senior Agency Official for Privacy (SAOP)

The SAOP is responsible for ensuring GSA's compliance with privacy laws, regulations and GSA policy, and the privacy control baseline in NIST SP 800-53. The SAOP designates which privacy controls can be treated as common and hybrid. The SAOP, or designated Privacy Analyst, reviews authorization packages and signs Certification Letters to verify compliance with applicable privacy requirements and to manage privacy risks prior to authorizing officials making risk determination and acceptance decisions.

### 1.5.6 GSA Chief Privacy Officer (CPO)

The CPO is responsible for overseeing GSA's Privacy Program, whose mission is to preserve and enhance privacy protections for all individuals whose personal information is handled by GSA and to encourage transparency of GSA operations involving personal information. The CPO manages GSA's Privacy Act Program and administers GSA's compliance with privacy laws and regulations. The CPO is responsible for developing, managing, and administering GSA's Privacy Program Plan and Privacy Strategy Plan.

### 1.5.7 Privacy Analysts

Privacy Analysts are responsible for ensuring implementation of adequate privacy for a system in order to document, mitigate, and minimize the privacy risks associated with collecting, using, processing, storing, maintaining, and disseminating PII. A Privacy Analyst must be assigned for every information system that contains PII and may have responsibility for more than one system, provided there is no conflict. The Privacy Analyst must be knowledgeable of the PII and processes supported by their assigned systems. Privacy Analysts, when delegated, review and sign Certification Letters, and oversee proper implementation of privacy controls. Privacy Analysts review PTAs/PIAs for their assigned systems.

### 1.5.8 Heads of Services and Staff Offices (HSSOs)

HSSOs are responsible for authorizing the operation of all systems, networks, and applications for which they have responsibility. They may delegate some of their authority (e.g., the role of Authorizing Official in writing) to appropriately qualified individuals within their organizations.

### 1.5.9 Authorizing Officials (AOs)

AOs are responsible for authorizing the operation of all systems, networks, and applications for which they have responsibility. They may delegate some of their authority (e.g., the role of Authorizing Official in writing) to appropriately qualified individuals within their organizations.

### 1.5.10 Office of CISO Division Directors

OCISO Directors are the intermediary to the AO for ensuring IT security is properly implemented. The Directors are GSA's points of contact for all IT system security matters for the IT resources under their responsibility.

### 1.5.11 Information System Security Managers (ISSMs)

ISSMs report to the ISSO Support Division (ISC) Director in the OCISO. There is at least one ISSM per AO. The ISSM is responsible for all IT system security and privacy matters for the systems under their authority. ISSMs work with ISSOs, System Owners, AOs, and others as security and privacy controls are implemented and review A&A packages for systems under their purview. ISSMs are appointed, in writing, by the Director of ISC with concurrence by the CISO. An individual appointed as an ISSM for a system cannot also be assigned as the ISSO for the same system.

### 1.5.12 Information System Security Officers (ISSOs)

ISSOs are responsible for ensuring implementation of adequate system security and privacy protections, including proper control implementations, in order to manage cybersecurity risk aligned with the NIST CSF functions of Identify, Protect, Detect, Respond, and Recover. An ISSO must be assigned for every information system. An ISSO may have responsibility for more than one system, provided there is no conflict. An individual assigned as the ISSO for a system cannot also be the ISSM for the same system. ISSOs must be appointed via a designation letter. An ISSO must be knowledgeable of the information and processes supported by their assigned systems. ISSOs review A&A packages for systems under their purview.

### 1.5.13 System Owners

System Owners are management officials within GSA who bear the responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's IT systems. System Owners represent the interests of the system throughout its lifecycle. Primary responsibility for managing risk rests with the System Owners. System Owners must ensure their systems and the data each system processes have the necessary security and privacy controls in place and are operating as intended and protected IAW GSA regulations and any additional guidelines established by the OCISO and relayed by the ISSO or ISSM.

### 1.5.14 Data Owners (i.e., Functional Business Line Managers)

Data Owners are responsible for determining the security categorization level of systems based upon FIPS Publication 199, “Standards for Security Categorization of Federal Information and Information Systems,” and ensuring System Owners are aware of the sensitivity of data (e.g., Personally Identifiable Information, Controlled Unclassified Information) to be handled. They must coordinate with System Owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, protected, and monitored IAW GSA policies, regulations and any additional guidelines established by GSA.

### 1.5.15 Contracting Officers (COs)/Contracting Officer’s Representatives (CORs)

COs/CORs are responsible for coordinating and collaborating with the CISO or other appropriate officials to ensure all agency contracts and procurements are compliant with the agency’s information security policy. They also must ensure the appropriate security and privacy contracting language is incorporated in each contract and task order.

Contracting language is specified in CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts, the current version is available on the IT Security Procedural Guides Insite Page. All GSA contracts with IT managed services (e.g., development, O&M, etc.) are to be submitted for IS review of the security and privacy language via the IS Contract Review Google Form.

### 1.5.16 Custodians

Custodians own the hardware platforms and equipment on which the data is processed. They are the individuals in physical or logical possession of information from Data Owners. They must coordinate with Data Owners and System Owners to ensure the data is properly stored, maintained, and protected.

### 1.5.17 Users of IT Resources

Authorized users of GSA IT resources, including all Federal employees and contractors, either by direct or indirect connections, are responsible for complying with GSA’s IT Security Policy and procedures.

### 1.5.18 System/Network Administrators

System/Network Administrators are responsible for ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines.

### 1.5.19 OCISO DevSecOps Program (ODP) Security Engineers

ODP Security Engineers are responsible for collaborating with the system team on all aspects of system security and acting as liaison with the OCISO for security decisions and approvals.

## 2 Identifying Appropriate ATU or ATO Process

The next two sections list GSA’s ATU and ATO processes along with applicability/qualifying criteria to use a specific process. The applicability/qualifying criteria listed in Tables 2-1 and 2-2

identify the conditions under which each process may be used. If additional guidance is necessary or there is a question about which process to use, contact any GSA ISSM, the ISA, or the ISC Director, to determine the appropriate process to follow.

## 2.1 Identifying the Appropriate ATU Process

Table 2-1 identifies the applicability/qualifying criteria for GSA's ATU processes.

**Table 2-1. GSA ATU Processes**

| ATU Process | Applicability/Qualifying Criteria |
|---|---|
| **GSA Salesforce Platform** (See Section 3.1) | • Salesforce Organizations that integrate into GSA's Salesforce Force.com platform and are hosted on Salesforce.com's infrastructure.<br>• Applications developed for internal and external GSA use published on the GSA's Salesforce Force.com platform. |
| **GSA Pages Site Review** (See Section 3.2) | • Sites hosted on the GSA Pages platform. |
| **Robotic Process Automation (RPA)** (See Section 3.3) | • Bots used to interact with GSA systems. |
| **Chrome Extensions** (See Section 3.4) | • Google Chrome browser extensions for use within GSA. |
| **SaaS Add-ons** (See Section 3.5) | • A marketplace SaaS add-on used to enhance the functionality of the host platform. |
| **Google Apps Scripts** (See Section 3.6) | • Google Apps scripts for use within GSA. |
| **Google Cloud Platform (GCP) Services** (See Section 3.7) | • Google Cloud Platform (GCP) services not currently Federal Risk and Authorization Management Program (FedRAMP) approved. |
| **AWS Services** (See Section 3.8) | • Amazon Web Services (AWS) services not currently FedRAMP approved. |

## 2.2 Identifying the Appropriate ATO Process

Table 2-2 identifies the applicability/qualifying criteria for GSA's ATO processes.

**Table 2-2. GSA ATO Processes**

| ATO Process | Applicability/Qualifying Criteria |
|---|---|
| **GSA Standard A&A Process**<br><br>(See Section 5) | • All new and existing GSA information systems that do not fall under one of the other A&A processes. |

| ATO Process | Applicability/Qualifying Criteria |
|---|---|
| **Lightweight Security Authorization Process** (See Section 4.2) | • New GSA application.<br>• Reside on infrastructures that have a GSA ATO concurred to by the CISO or a FedRAMP infrastructure as a service (IaaS) provisional ATO.<br>• Must be FIPS 199 Low or Moderate.<br>• Prior to pursuing a Limited Authorization to Operate (LATO) using this process the GSA CISO must approve its use. |
| **Low Impact Software as a Service (LiSaaS) Solutions Authorization Process** (See Section 4.3) | • Cloud computing Software as a Service (SaaS) solutions that are implemented within GSA.<br>• Will not be used in a permanent capacity at GSA (implemented for a limited duration).<br>• Involve data already in the public domain or data is non-sensitive and determined to be FIPS 199 Low impact.<br>• Could cause limited harm to GSA regardless of the consequence of an attack or compromise.<br>• Have a cost for deployment not exceeding $100,000 annually.<br>• Will not impact operations or business processes should they experience a disruption in service or the inability to access the service.<br>• Risk level of the LiSaaS solution will be determined through completion of a LiSaaS Solution Profile and LiSaaS Solution Review Checklist available on the InSite IT Security Forms and Aids web page. |
| **GSA Agency FedRAMP Process** (See Section 4.4) | • A CSP requesting GSA Agency sponsorship into FedRAMP.<br>• GSA accepts sponsoring the CSP.<br>• GSA determines CSP's security authorization package will be considered FedRAMP compliant. |
| **Moderate Impact Software as a Service (MiSaaS) Security Authorization Process** (See Section 4.5) | • New GSA information systems.<br>• Reside on infrastructures that have, or are pursuing, a Federal Risk and Authorization Management Program (FedRAMP) ATO.<br>• Must be FIPS 199 Moderate.<br>• Prior to pursuing a MiSaaS ATO using this process the GSA CISO must approve its use. |
| **GSA Subsystem Process** (See Section 4.6) | • Classified as a subsystem (and not a Salesforce application).<br>• Dependent upon resources provided by its supporting FISMA system.<br>• FIPS 199 Low or Moderate.<br>• FIPS 199 level may be equal to or below the level of the supporting FISMA system. |
| **GSA Ongoing Authorization (OA) Program** (See Section 4.7) | • The information system must have had all its NIST SP 800-53 security controls for its applicable FIPS 199 level, and any additional controls required by the GSA CISO assessed within the past 18 months and issued an ATO.<br>• The information system must have deployed GSA's enterprise ISCM tools, based on applicable system requirements, defined within the GSA ISCM Enterprise Security Management Tools. |

| ATO Process | Applicability/Qualifying Criteria |
|---|---|
| **GSA Leveraged FedRAMP SaaS Solution Process** (See Section 4.8) | • Leveraged SaaS must have a FedRAMP ATO.<br>• All customer responsibilities in the CSP's Customer Responsibility Matrix (CRM) must be addressed in a CRM SSP.<br>• Must be FIPS 199 Low or Moderate. |
| **GSA Mobile Application Review and Approval Process** (See Section 4.9) | • Mobile applications (apps) in use at GSA or that are part of a system boundary.<br>• Mobile apps must be assessed and approved as standalone or as part of a system boundary. |
| **GSA High Value Asset (HVA) Approval Process** (See Section 4.10) | • Systems determined to be HVAs IAW the process in CIO-IT Security-26-148: Managing High Value Assets.<br>• HVAs follow the GSA Standard A&A Process (Section 5), however they must include the HVA Overlay controls to their baseline as described in Section 4.10. |

# 3 ATU Process Summaries

Additional details about the GSA ATU processes listed in Table 2-2 are provided in the following sections.

## 3.1 GSA Salesforce Platform Process

- **Document Reference:** CIO-IT Security-11-62: Salesforce Platform Security Implementation
- **Result:** Salesforce Organization or Application ATU
- **Summary of Process**: Specific to Salesforce Organizations and applications developed for internal and external GSA use published on GSA's Salesforce Force.com platform. Organizations and applications are approved for use based on implementation of NIST SP 800-53 controls, security configuration settings, user permissions, and completing the ATU process as detailed in CIO-IT Security-11-62.
- **Approval Process**: After the ISSM accepts/approves the ATU package it becomes a part of the SSP and allows the application to be added to the Salesforce inventory along with POA&Ms reflecting any identified vulnerabilities.

## 3.2 GSA Pages Site Review and Approval Process (formerly Federalist Site Process)

- **Document Reference**: CIO-IT Security-20-106: GSA Pages Site Review and Approval Process
- **Result**: GSA Pages Site ATU
- **Summary of Process**: Each request to approve hosting a static site on the GSA Pages platform must include a completed GSA Pages Site Review and Approval Template. A Google Form for GSA Website Managers must also be submitted. Site URLs currently hosted on the GSA Pages platform must be scanned in accordance with GSA's parameter for NIST SP 800-53 control RA-05, Vulnerability Scanning, and as described in Section 9.3.4.

- **Approval Process**: After reviewing the completed artifacts, the ISSM may approve the site for hosting. Sites with Critical or High security findings will not be approved. The GSA Website Manager signs the completed GSA Pages Site Review and Approval Template and agrees to follow the GSA Pages system wide IR and CM plans.

## 3.3 RPA Process

- **Document Reference**: CIO-IT Security-19-97: Robotic Process Automation (RPA) Security.
- **Result**: RPA ATU
- **Summary of Process**: Each request to approve a GSA RPA Bot must include a completed Privacy Threshold Assessment (PTA) to determine if a Privacy Impact Assessment (PIA) is required and a completed RPA Attributes Questionnaire, which includes questions/requirements based on the type of bot (i.e., simple, complex), rules of behavior, and interaction with systems. If an API is involved with the Bot process, the API information must be included in a Process Design Document (PDD) or a completed API Security Questionnaire.
- **Approval Process**: After reviewing the questionnaire and required artifacts, the RPA ISSO may approve simple bots. After reviewing the questionnaire and required artifacts for complex bots, the RPA ISSO relays them to the RPA ISSM for approval.

## 3.4 Chrome Extensions

- **Document Reference**: Google Workspace – Chrome - Extensions
- **Result**: Addition to the lists of GSA Approved/Rejected Extensions
- **Summary of Process**: Each request for a Chrome Extension must follow the process described at Chrome Extension Request. Requests for new extensions (i.e., those not already approved or rejected) require a Service Catalog request.
- **Approval Process**: Service Catalog requests for new extensions are routed to the OCISO C-SCRM Team (ISA) for review. After ISA completes the review, the approved/rejected lists are updated, and the requestor notified along with rationale if rejected.

## 3.5 SaaS Add-ons

- **Document Reference**: SaaS Add-On Request
- **Result**: Addition to the lists of GSA Approved/Rejected SaaS Add-ons
- **Summary of Process**: A marketplace SaaS add-on is a third-party application, extension, plugin, or integration that is discovered, purchased, and installed through an existing GSA SaaS provider's centralized marketplace (e.g., Salesforce, AppExchange, Google Add-ons) to enhance the functionality of the host platform. Each platform will have its own guidelines for approval. Requests for SaaS add-ons must follow the process described at SaaS Add-On Request Requests for new SaaS add-ons (i.e., those not already approved or rejected) require a Service Catalog request.

- **Approval Process**: Service Catalog requests for new SaaS add-ons are routed to the OCISO C-SCRM Team (ISA) for review. After the request is reviewed by stakeholders, the approved/rejected lists are updated, and the requestor notified along with rationale if rejected.

## 3.6 Google Apps Scripts

- **Document Reference**: Google Workspace App Script
- **Result**: Google App Script ATU
- **Summary of Process**: Externally developed scripts are prohibited but may be allowed following OCISO review. Internally developed scripts are implicitly allowed but require review by the OCISO and may be restricted from use pending the results of the review. Internally developed scripts must follow the GSA naming convention as described in GSA Order CIO 2100.1.
- **Approval Process**: Use the Google App Script Approval Form to request approval for internal and external scripts. After ISB completes its review, the script will be approved or rejected, and the requestor notified along with the rationale if rejected.

## 3.7 GCP Services

- **Document Reference**: IS-GCP Services Tracking Sheet (see GCP Service Review Process Tab)
- **Result**: GCP (Non-FedRAMP) Services ATU
- **Summary of Process**: Specific to GCP services not currently FedRAMP approved. Requestors must provide the following details to ISB in order to request GCP services:
  - GCP Service Name;
  - Short Service Description; and
  - Core Security Information (see Google Cloud- Cloud Service Review Template for details).
- **Approval Process**: Requests for GCP services to be reviewed should be submitted to seceng@gsa.gov. ISB will approve or reject the GCP service based on a security review of the service. Approved services may require additional usage conditions/restrictions for use at GSA.

## 3.8 AWS Services

- **Document Reference**: IS Master AWS Services Tracking List (see About This Sheet Tab)
- **Result**: AWS (Non-FedRAMP) Services ATU
- **Summary of Process**: Specific to AWS services not currently FedRAMP. Requestors must provide the following details to ISB in order to request AWS services:
  - AWS Service Description;
  - AWS Service Name; and
  - Core Security Information (see IS AWS Service Template for details).

- **Approval Process**: Requests for AWS services to be reviewed should be submitted to seceng@gsa.gov. ISB will approve or reject the AWS service based on a security review of the service. Approved services may require additional usage conditions/restrictions for use at GSA.

# 4 A&A Process Summaries

GSA's different A&A processes have been developed to ensure the risks to operating GSA IT systems and their data are reduced to the extent possible based on budget constraints, business requirements and other resource issues. For all A&A processes (except for a 90-day LATO) before assessment activities for an information system can begin, the following requirements must be met:

(1) The information system must be clearly defined in an SSP or LiSaaS Profile/Checklist. **Note**: An SSP is not required for the 90-day LATO process.
(2) The information system's architecture must be approved by the ISB Division.
(3) A SAP (or other method of assessment when a SAP is not required) must be approved.

To assist ISSOs and/ISSMs in managing recurring tasks regarding A&A processes and the security of GSA information systems Federal and Contractor ISSO Checklists have been developed in GSA's GRC tool.

Any GSA system leveraging a FedRAMP authorization must provide a copy of the GSA ATO Letter to the FedRAMP Program Management Office (PMO). ISSOs must coordinate with their ISSM to ensure the FedRAMP PMO receives notification.

Additional details about the GSA ATO processes listed in Table 2-2 are provided in the following sections.

## 4.1 GSA Standard A&A Process

- **Document Reference**: Section 5 of this guide.
- **Result**: Standard ATO.
- **Summary of Process**: All new and existing GSA information systems, except systems in Ongoing Authorization must undergo a security A&A at least every three (3) years or whenever there is a significant change to the system's security posture. The result is an ATO for a period not to exceed three (3) years. Specific requirements are detailed throughout this guide.
- **Approval Process**: Follows the process described in Section 5.6.4, Authorization Decision.

## 4.2 Lightweight Security Authorization Process

- **Document Reference:** CIO-IT Security-14-68: Lightweight Security Authorization Process.
- **Result**: 90 day LATO, 1 Year LATO (Moderate); 3 Year ATO (Low)
- **Summary of Process:** Prior to pursuing a LATO using the Lightweight process the GSA CISO must approve its use. New GSA information systems residing on infrastructures

that have a GSA ATO concurred by the GSA CISO or a FedRAMP IaaS ATO are eligible. The process supports the following ATOs.

A 90-day LATO can be issued based on the results of a limited assessment (e.g., vulnerability scans, penetration tests). See Appendix D for the documents required to issue a 90-day LATO.

A one-year LATO (for FIPS 199 Moderate) or a three-year ATO (for FIPS 199 Low) can be issued based on completing the full lightweight security authorization process described in CIO-IT Security-14-68. See Appendix D for the documents required to issue a one year ATO.

- **Approval Process**: Follows the process described in Section 5.6.4, Authorization Decision.

## 4.3 Low Impact Software as a Service (LiSaaS) Solutions Authorization Process

- **Document Reference:** CIO-IT Security-16-75: Low Impact Software as a Service (LiSaaS) Solutions Authorization Process.
- **Result:** No more than one year if the application is determined to be Low Risk, or up to three years if the application is determined to be a commodity, ancillary service that presents Very Low/Negligible risk.
- **Summary of Process:** Process is for cloud computing Software as a Service (SaaS) solutions that (1) will not be utilized in a permanent capacity at GSA (implemented for a limited duration); (2) involve data already in the public domain or data that is non-sensitive and determined to be FIPS 199 low impact; (3) could cause limited harm to GSA regardless of the consequence of an attack or compromise; (4) have a cost for deployment not exceeding $100,000 annually; and (5) will not impact operations or business process should they experience a disruption in service or the inability to access the service. To request a LiSaaS software review for software not already approved a GSA ServiceNow Service Catalog Software Review Request must be submitted.

  To receive an ATO a LiSaaS solution must complete the following actions to document the system and the risk of its use:

  - Complete a LiSaaS Solution Profile.
  - Complete a LiSaaS Solution Review Checklist.
  - Document how system and security parameters deferred to customers are implemented.
  - Provide vulnerability scan results.
  - Have no Critical or High vulnerabilities identified in their scans.
  - Document an acceptable flaw remediation process.
  - Provide sufficient information to understand the solution's security posture and operating risk. The basic requirement is an audit report (e.g., Service Organization Control [SOC] 2/Statements on Standards for Attestation Engagements [SSAE] 18) or a certification (e.g., Systrust, WebTrust, etc.); however, the GSA AO and the CISO will take a holistic view of the application based on all documentation presented to determine the overall risk of using the application.

  See Appendix D for the documents required to issue a LiSaaS ATO. Any LiSaaS solution granted a one year LiSaaS ATO must obtain a FedRAMP Tailored (at a

minimum) authorization within one year of its ATO. Detailed information on the entire process is available in CIO-IT Security-16-75.

- **Approval Process**: Follows the process described in Section 5.6.4: Authorization Decision.

## 4.4 GSA Agency FedRAMP Authorization Process

**Document Reference:** FedRAMP Agency Authorization webpage. GSA is developing an IT Security Procedural Guide: OCISO FedRAMP Program to define the process by which a GSA agency authorization can be achieved.

- **Result**: FedRAMP ATO (Agency)
- **Summary of Process**: A CSP, through a GSA business line, may request that GSA support the CSP through the Agency FedRAMP ATO process in efforts to achieve an ATO from GSA. It is at the discretion of GSA to accept or deny the CSP's request for sponsorship. CSPs which GSA agrees to sponsor for a FedRAMP authorization are required to follow the FedRAMP PMO authorization process requirements. CSPs must follow the FedRAMP CTW, guidance will be provided by GSA regarding requirements FedRAMP leaves for an Agency to define. Additional information about FedRAMP is available in the reference documents and at the FedRAMP webpage. The CSP must work with GSA throughout the entire authorization, providing requested artifacts at various checkpoints and receiving incremental approval, and ultimately delivering a completed security authorization package to GSA. If GSA determines the package to be FedRAMP compliant, the CSP in cooperation with GSA will pursue a FedRAMP ATO.

  System Owners/AOs with questions about using the FedRAMP security authorization process (to attain a Government wide authorization) should contact the OCISO at ociso.fedramp@gsa.gov.

## 4.5 Moderate Impact Software as a Service (MiSaaS) Security Authorization Process

- **Document Reference:** CIO-IT Security-18-88: Moderate Impact Software as a Service (MiSaaS) Security Authorization Process.
- **Result:** 1 Year ATO
- **Summary of Process:** Prior to pursuing an ATO using the MiSaaS process the GSA CISO must approve its use. New GSA information systems residing on infrastructures that have, or are pursuing, a FedRAMP ATO. The process allows for a FIPS 199 Moderate impact SaaS to be granted a one-year ATO after completing the tailored RMF process detailed in CIO-IT Security-18-88.

  See Appendix D for the documents required to issue a MiSaaS ATO.
- **Approval Process:** Follows the process described in Section 5.6.4, Authorization Decision

## 4.6 GSA Subsystem Process

- **A&A Process Reference:** Described within this section.
- **Result:** ATO aligned with subsystem's supporting FISMA system.

- **Summary of Process:** This process is specific to subsystems (other than Salesforce applications) which are: (1) categorized with a FIPS 199 security impact level of Low or Moderate; and (2) dependent upon the resources provided by its supporting FISMA system. The supporting FISMA system must be shown to provide a foundational level of protection for the subsystem; the subsystem may have a FIPS 199 level equal to or below the level of its supporting FISMA system.

  Subsystems must identify and tailor the controls they are responsible for as they are scoping their boundary. Subsystems will document all controls where the subsystem has either hybrid or system specific requirements in its SSP. These controls will be assessed using GSA's NIST 800-53 Test Cases and the results shared with the supporting FISMA system's System Owner/ISSO. All subsystems will be identified in Appendix C of their supporting FISMA system's SSP and will be listed in the hosting/supporting system's ATO Letter. All subsystems inherit its supporting FISMA system's ATO cycle.

- **Approval Process**: New and transferred subsystem ATOs align to their parent. Existing subsystems (and new and transferred when added) are included in the A&A Package review and approval process of their parent FISMA system.

## 4.7 GSA Ongoing Authorization (OA) Program

- **A&A Process Reference:** CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program.
- **Result:** Ongoing Authorization to Operate (OATO)
- **Summary of Process:** GSA has implemented its OA Program as summarized below.
  - A system must meet the OA prerequisites identified in CIO-IT Security-12-66.
    - The information system must have had all its NIST SP 800-53 security controls for its applicable FIPS 199 level, and any additional controls required by the GSA CISO assessed within the past 18 months and issued an ATO.
    - The information system must have deployed GSA's enterprise security tools, based on applicable system requirements, defined within the GSA ISCM Enterprise Security Management Tools.
    - The information system must be compliant with all Critical controls as identified in Appendix B.
    - The information system must be compliant with CISA BODs and EDs.
  - An OA Onboarding Checklist is completed by the OA Team in collaboration with the ISSO, ISSM, and system team. The OA checklist reviews five main security areas including ISCM/CDM Tools, Vulnerability Management, Configuration Compliance, Critical Security Controls and Security Documentation.
  - An Onboarding Assessment Report (OAR) is prepared by the OA Team and ISSO. The OAR is functionally the SAR for systems entering the OA Program.
  - Systems suitable for OA have an Onboarding Approval Meeting (OAM) held with the OA Team and system personnel.
  - OATO Letter is prepared and routed for signature.
  - Systems in OA undergo biannual performance metric reviews (PMRs) with results presented to the CISO and AO to make a risk-based determination on continuance in the OA program. Additional details are available in CIO-IT Security-12-66.

- **Approval Process**: Follows the same process described in Section 5.6.4, Authorization Decision, with the following exception: the Director of ISA replaces the Director of ISC.

## 4.8 GSA Leveraged FedRAMP SaaS Solution Process

- **A&A Process Reference:** Described within this section.
- **Result:** ATO for a Leveraged FedRAMP SaaS Solution
- **Summary of Process:** GSA's process for issuing an ATO leveraging a FedRAMP SaaS solution is as described below. Every instance of a leveraged solution needs its own ATO unless the ATO is for a GSA enterprise solution (e.g., Google Workspace).

  Leveraged SaaS documentation, assessment, and authorizations will be limited to the GSA control baseline authorization target. Customer responsibilities identified by FedRAMP authorized CSPs that are above and beyond the GSA implemented FIPS impact level baseline are recommended but not required to be documented, assessed, and authorized in GSA Leveraged SaaS implementations.

  Any evidentiary artifacts or documents supporting the implementation status determination must be stored in a central location for review.

  1. **SSP Requirements**: A CRM SSP is developed documenting the leveraged solution and GSA's implementation of the customer responsibilities listed in the CSP CRM for the solution. A CRM SSP Template is available on the InSite IT Security Forms and Aids web page. Other documents required in support of an ATO are:
     - A FIPS 199 Security Categorization identifying the information types GSA will use with the leveraged solution.
     - A PTA to identify if any Personally Identifiable Information (PII) is used with the leveraged solution. If PII is used, a PIA will also be required.
     - A DIAS identifying the Identity, Authentication, and Federation Assurance Levels required for the leveraged solution.
     - Other documents may be required based on CSP's CRM.
  2. **Security Assessment Requirements:** Assessments are conducted in relation to the CRM controls/requirements and test cases must be tailored to these requirements. Assessment evidence consists of the artifacts supporting the implementation status determinations.

  **FIPS 199 Low and Moderate Impact SaaS (without PII)**

  - The FedRAMP authorized SaaS does not require independent assessment.
  - A CRM SAR Attestation of CRM controls must be prepared by the ISSO and ISSM and verified by the ISC Director. A CRM SAR Attestation template is available on the IT Security Forms and Aid page.
  - As an interim process until GSA's GRC tool supports CRM SAR assessments, the following process may be used. The CSP CRM is updated by adding four columns to the right of the last column in the customer responsibility matrix tab. The columns are to be labeled as listed below. Complete the columns for all the responsibilities listed.
    - Implementation Status (Yes/No).
    - Comments (If any/applicable).

- Deviation – deviations must include artifact(s) on an alternative implementation or other rationale for the deviation.
- Artifacts (link to artifact(s) supporting implementation status).

**FIPS 199 Moderate Impact SaaS (with PII)**

- The FedRAMP authorized SaaS must be independently[1] assessed against the CSP-identified CRM controls.
- A Security Assessment Report (SAR) must be prepared documenting the results of the assessment.

3. **Authorization Package Requirements:** See Appendix D for the documents required to receive a Leveraged FedRAMP ATO.
4. **Leveraged SaaS Authorization Approval Process:** After review of the security authorization package, an ATO letter is prepared, which may be an update to an existing ATO letter for a system/platform. Templates are available on the InSite IT Security Forms and Aids web page. A copy of the ATO Letter must be provided to the FedRAMP PMO. The ISSO and ISSM will coordinate delivery to FedRAMP.
5. **Maintaining Leveraged SaaS ATOs:** Leveraged SaaS ATOs must be updated when the following activities occur.
   - The CSP updates the Leveraged SaaS' CRM.
   - GSA's implementation of the Leveraged SaaS has changed (e.g., services or functionalities added or modified).
   - A security incident occurred that included a corrective action plan.

   An assessment must be conducted as specified in Section 5.7.4.

   Annually, an attestation must be completed to validate the Leveraged SaaS' ATO is still valid (i.e., none of the conditions above apply) or one of the conditions applies and a new ATO is issued.

## 4.9 GSA Mobile Application Review and Approval Process

- **Document Reference:** CIO-IT Security-12-67: Securing Mobile Applications and Devices.
- **Result**: Mobile App is added to the Allowed List and/or GSA designed Mobile App is integrated into a supporting system's SSP and ATO boundary.
- **Summary of Process**: Developed applications or Commercial-off-the-Shelf (COTS) applications may be added to GSA's Allowed list after successfully completing the processes defined in CIO-IT Security-12-67 which is summarized below.
  - A user or System Owner/custodian submits a Mobile App Allowlist Request.
  - The Mobile App goes through the assessment processes defined in CIO-IT Security-12-67.
  - If the Mobile App's business use case is approved, it is added to the Allowed List; or

[1] Independence is defined as when assessors do not: (i) have a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are assessing; or (iv) place themselves in positions of advocacy for the organizations acquiring their services.

  - If the Mobile App supports a GSA information system, the system's SSP must be updated and a delta assessment of the mobile application must be completed

- **Approval** Process: Follows the process described in CIO-IT Security-12-67

### 4.10 GSA High Value Asset (HVA) Approval Process

- **Document Reference:** CIO-IT Security-26-148: Managing High Value Assets.
- **Result:** ATO for an HVA system.
- **Summary of Process:** After a system is determined to be an HVA the following process is followed.
  - The HVA Overlay controls are applied to the system's FIPS 199 Baseline (Moderate or High).
    - If the system's baseline does not include a NIST control that is in the HVA Overlay, the control is added to the system's baseline.
    - If the system's baseline includes a NIST control that is in the HVA Overlay, the baseline control is replaced by the HVA Overlay control, including the HVA parameters.
  - The HVA SSP (Moderate or High) template is used to document the HVA system's control implementations.
  - The HVA test case workbook (Moderate or High) is used to assess the system's control implementations.
- **Approval Process:** Follows the process described in Section 5.6.4, Authorization Decision.

## 5 GSA Standard A&A Process

All GSA A&A processes are based upon NIST SP 800-37. A depiction of the NIST RMF steps is provided in Figure 5-1.

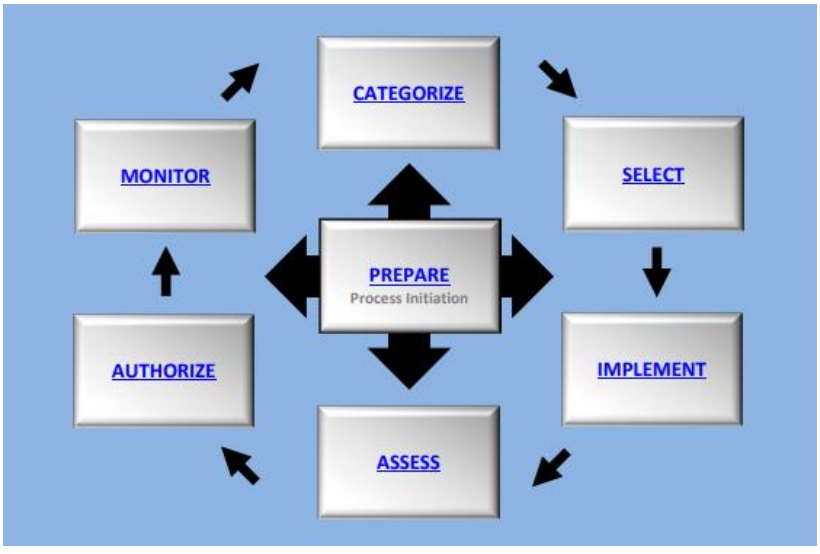


**Figure 5-1. Risk Management Framework Steps (from NIST 800-37, Revision 2)**

The RMF steps associated with the GSA Standard A&A Process are detailed in the following sections. Additional A&A processes GSA has developed or uses are identified in Section 4 which have been adapted or modified from the standard RMF processes.

The RMF steps in this section are documented in their sequential order from NIST SP 800-37. Similar to NIST SP 800-37, after the Prepare step the RMF steps may be completed in a non-sequential order due to the system type, the life cycle stage, and development process (e.g., agile development often generates multiple iterations of steps). When systems are in the Monitor step, changes to the system may cause multiple steps to be revisited. In addition, tasks in some steps may occur concurrently for efficiency. For example, in the Select step, the control selection, control tailoring, and some aspects of control allocation are interrelated which may benefit by considering them at the same time.

As required by EO 13800, GSA has aligned its risk management process with the CSF 2.0. The six core CSF 2.0 Functions are:

- **Govern (GV):** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- **Identify (ID):** The organization's current cybersecurity risks are understood.
- **Protect: (PR):** Safeguards to manage the organization's cybersecurity risks are used.
- **Detect (DE):** Possible cybersecurity attacks and compromises are found and analyzed.
- **Respond (RS):** Actions regarding a detected cybersecurity incident are taken.
- **Recover (RC):** Assets and operations affected by a cybersecurity incident are restored.

Appendix C contains a mapping of the NIST RMF steps and tasks to the six core functions of the CSF 2.0 in Table C-1. Table C-2 provides the definitions for the CSF 2.0 Categories and Subcategory Unique Identifiers.

## 5.1 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."

### Organization Level Prepare Tasks

Additional details on the organizational prepare steps described in the following sections are included in CIO-IT Security-18-91: Risk Management Strategy (RMS), CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC), CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program, CIO 2100.1, and guides describing GSA's various A&A processes identified in Section 4.

### 5.1.1 TASK P-1: Risk Management Roles

CIO 2100.1, Section 1.5 of this guide, and CIO-IT Security-18-91: Risk Management Strategy (RMS) identify and assign key roles for executing the RMF within GSA. The CISO, Authorizing Officials, SAOP, ISSMs, ISSOs, System Owners, the Privacy Office, and subject matter experts from the OCISO and other GSA organizations facilitate the consistent application of cybersecurity risk management across GSA.

### 5.1.2 TASK P-2: Risk Management Strategy

The EMB, chaired by the Deputy Administrator who is also the SAORM manages enterprise risk at GSA. For cybersecurity risks, the ERES, co-led by the Deputy Performance Improvement Officer and the CISO, identifies and monitors agency-wide risks and ensures the EMB is updated on the risks and impacts to GSA. CIO-IT Security-18-91: Risk Management Strategy provides a comprehensive approach for framing, assessing, responding to, and monitoring risks associated with GSA information systems in accordance with Federal laws, regulations, and requirements. It addresses risk tolerance, determination, acceptance, mitigation, and communication within GSA and to external organizations. The GSA Privacy Program addresses privacy risks at GSA.

### 5.1.3 TASK P-3: Risk Assessment – Organization

The EMB along with the ERSI address risks at the organizational level. The EMB meets periodically at the direction of the Deputy Administrator (Chair) or the Chief Financial Officer/Performance Improvement Officer (Deputy Chair) to assess and update organizational risks at GSA. CIO-IT Security-18-91: Risk Management Strategy contains additional details about the EMB and ERSI.

### 5.1.4 TASK P-4: Organizationally – Tailored Control Baselines and Cybersecurity Framework Profiles

Tailored baselines at GSA are established by:

1. Determining a system's FIPS 199 Security Categorization (i.e., Low, Moderate, or High).
2. Identifying the GSA A&A process the system will follow (see Section 4).
3. Using the GSA Control Tailoring Workbook (CTW) to identify the system's initial tailored control baseline.
4. Determining if any of GSA's control overlays apply to the system based on the conditions indicated below and applying them to establish the system's final control baseline.
    - Privacy Overlay - system contains, transmits, or processes PII.
    - CUI Overlay - system contains, transmits, or processes CUI.
    - HVA Overlay - system has been designated an HVA.
    - PCI Overlay - system boundary includes assets that contain, transmit, or process PCI data.
    - Infrastructure Overlay - system includes infrastructure components (e.g., networking assets, monitoring assets, physical assets).

### 5.1.5 TASK P-5: Common Control Identification

GSA IT Security-18-90: Common Control Catalog (CCC) identifies enterprise-wide common and hybrid controls. It provides implementation details about common controls and common portions of hybrid controls for systems to inherit, and information regarding system responsibilities for the hybrid controls.

The GSA is in the process of identifying the apportionment of controls for other common control sources such as GSA enterprise systems (e.g., general support systems, platforms) and other

SSO systems or sources. System Owners inheriting controls must ensure that providing systems agree that they are providing the controls and then document this inheritance in their SSPs. As the GSA moves SSPs into its GRC tool, control inheritance will be implemented such that common control providers will designate controls being provided and systems inheriting controls will identify controls they are inheriting and the systems they are inheriting them from. As this information becomes available in GSA's GRC tool some of the manual activities discussed will happen automatically.

Common control providers are responsible for:

- documenting common controls in an SSP (or equivalent document prescribed by the organization);
- ensuring that common controls are developed, implemented, and assessed for effectiveness by qualified assessors with a level of independence required by the organization;
- documenting assessment findings in a security assessment report;
- producing a POA&M for all common controls deemed less than effective (i.e., having unacceptable weaknesses or deficiencies in the controls);
- receiving authorization for the common controls from the AO; and
- monitoring common control effectiveness on an ongoing basis.

The common control provider's SSP, Security Assessment Report (SAR), and POA&M for common controls (or a summary of such information) should be made available to System Owners (whose systems are inheriting the controls) after the information is reviewed and approved by the AO responsible and accountable for the controls.

A Control Implementation Summary (CIS) table based on the system's control baseline must be completed. The table identifies control types (common, hybrid, system specific), implementation status (Fully Implemented, Partially Implemented, Planned, etc.), and responsibility (OCISO, GSS/Platform/System) for the system's controls. The table should be customized to the GSA SSO or contractor's environment to account for additional designations of responsibility as necessary. CIS table templates are available for use on the InSite IT Security Forms and Aids web page.

The completed CIS table will be included as an attachment to the SSP. It will be updated in subsequent steps of the RMF process, including after security control implementation and following security assessment to document the results of the review.

### 5.1.6 TASK P-6: Impact-Level Prioritization

GSA has selected not to apply additional granularity to its systems as this optional task allows. GSA will continue to use a system's FIPS 199 security categorization of Low, Moderate, or High with no further priority or level within those categories. GSA has developed additional A&A processes, as listed in Section 4, which allows systems meeting the criteria for a specific process to streamline its A&A activities.

### 5.1.7 TASK P-7: Continuous Monitoring Strategy – Organization

The GSA continuous monitoring strategy leverages both manual and automated processes to monitor a system's security and privacy controls. The objective of the strategy is to ensure all key information security controls are periodically assessed for effectiveness. GSA's

organizational continuous monitoring strategy leverages its deployment of Continuous Diagnostics and Mitigation (CDM) and other GSA ISCM Enterprise Security Management Tools (e.g., Invicti, Enterprise Logging Platform) to monitor the security of GSA's systems. CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program provides more details on how GSA continuously monitors vulnerabilities, threats, and actions taken to reduce, mitigate, or eliminate them. Key components of GSA's strategy are regular vulnerability scanning activities and security configuration checks, the requirement to maintain A&A documents in an "as-is" state, management and review of POA&Ms, and ISSO Checklists within GSA's GRC tool.

## System Level Prepare Tasks

### 5.1.8 TASK P-8: Mission or Business Focus

The information system's missions, business functions, processes, and purposes the system is intended to support is to be documented in Section 9, General Description, of the GSA SSP template. The System Owner in collaboration with the ISSO completes this section of the SSP.

### 5.1.9 TASK P-9: System Stakeholders

The information system's system owner, AO, ISSO, ISSM, and other stakeholders (e.g., custodian, CSP, etc.) is to be documented in Sections 3-6 of the GSA SSP template. The System Owner in collaboration with the ISSO completes this section of the SSP.

### 5.1.10 TASK P-10: Asset Identification

The information system's assets, both tangible and intangible, are to be documented in Sections 8-10 of the GSA SSP template. Tangible elements include physical elements, human elements, and technological elements. Intangible elements include data/information, firmware, software, services, and processes/functions. For example, the assets would include the locations, types of information, hardware and software components, and users. The System Owner in collaboration with the ISSO completes this section of the SSP. As specified in GSA Order CIO 2160.1, "General Services Administration (GSA) Information Technology (IT) Standards Policy," GSA systems must only use software that has been approved and is listed on the GSA EA Analytics & Reporting (GEAR) website. The use of unlisted software may be requested via a ServiceNow Software Review Request.

### 5.1.11 TASK P-11: Authorization Boundary

The information system's authorization boundary is documented in Sections 9-11 of the GSA SSP template. The System Owner in collaboration with the AO and ISSO completes these sections of the SSP. The authorization boundary includes the system components, network architecture, and inventory. Diagrams showing connections and interconnections must clearly depict the authorization boundary. The tables for interconnections in the SSP must be completed, including agreements concerning those interconnections, as applicable.

CIO-IT Security 24-125: Managing Information Exchanges identifies the types of documentation and agreements required when GSA systems exchange information via different types of connections both internally (i.e., within GSA) and with external organizations (e.g., other Federal entities, companies).

### 5.1.12 TASK P-12: Information Types

The information system's information types are documented in Section 2 of the GSA SSP template. The data owner(s) and System Owner in collaboration with the ISSO completes this section of the SSP. A GSA FIPS 199 Security Categorization document must be completed and attached to the SSP. It will identify the information system types and overall security categorization of the system based on the information types listed in 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 Systems to Security Categories."

### 5.1.13 TASK P-13: Information Life Cycle

The life cycle of information must be described to include its creation or collection, processing, transmission, use, storage, and disposition. Sections 10.4 and 10.5 of the GSA SSP template must be completed to understand much of the information life cycle. Those sections describe how data flows within and into and out of the system. Other sections of the SSP, such as the Section 9 where the system missions, functions, and business processes must describe the collection or creation of information in order to fulfill the overall mission of the system. Specific controls regarding encryption of data and media protection and sanitization provide additional details on the transmission and disposition of information.

### 5.1.14 TASK P-14: Risk Assessment – System

An initial security assessment must be performed prior to a system receiving an ATO. This assessment includes assessing the risk of operating the system as detailed in the RMF Assess Step in Section 5.5 of this guide. Assessment of risk is also performed as part of the RMF Monitor Step in Section 5.7 of this guide.

### 5.1.15 TASK P-15: Requirements Definition

Completing the selection of the baseline and overlays required for a system in Task P-4 determines the security requirements/controls that the system must meet/implement. Any additional requirements/controls necessary for a system's business mission or environment will be coordinated by the System Owner with the AO, ISSM, ISSO, and Privacy Team in Task S-1.

### 5.1.16 TASK P-16: Enterprise Architecture

GSA's Office of Enterprise Architecture and Data Integration (IBC) in GSA IT is responsible for GSA's enterprise architecture. GSA Order CIO 2101.3, "GSA Integrated Information Technology Management" addresses enterprise architecture and its integration with the GSA IT Strategic Plan and GSA's Solution Lifecycle best practices in the GSA Solutions Life Cycle Handbook. The ISB Division works closely with other GSA IT Teams and other SSOs to facilitate integration of security standards/requirements into development efforts, ensuring secure outcomes as a matter of routine. Additional information is available in CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC) and the GSA EA Analytics & Reporting (GEAR) website.

### 5.1.17 TASK P-17: Requirements Allocation

Controls are allocated based on the common, hybrid, and system specific designations identified in CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC), GSA's various

A&A processes, the CTW, and SSP templates. GSA is also in the process of a control allocation mapping among its GSSs and Platforms to identify controls common or hybrid at those levels that systems can inherit. Allocation of controls to system components is the purview of the System Owner in collaboration with the OCISO.

### 5.1.18 TASK P-18: System Registration

System Owners, or their designated Program Managers and Project Managers, collaborate with the GSA SSOs as new systems are being considered for design, development, proof of concept, or implementation. GSA's ISSMs and ISSOs work closely with those offices and personnel to ensure systems are registered into the GSA system inventory as early as possible. ISSMs or designated personnel submit requests to add systems in GSA's official system inventory repository using the Agency System Inventory - FISMA Update Request Form and Agency System Inventory - Subsystem Update Request Form. GSA's GRC tool is the repository for GSA's system inventory. Systems are registered in it as soon as they are identified and are categorized as pending. They will stay in this status until they are placed into production.

## 5.2 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."

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

### 5.2.1 TASK C-1: System Description

The information system is described throughout Sections 1-12 of the GSA SSP template. The System Owner in collaboration with the ISSO completes these sections of the SSP. 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 SSP.

### 5.2.2 TASK C-2: Security Categorization

GSA's FIPS 199 Security Categorization Template or GSA's GRC tool is used to identify the information types handled by the system. Once the information types are determined the overall security categorization of the system is determined. This information is included in the system's SSP. NIST SP 800-60 Volumes I and II are used to identify the information types handled by the system. The result of the system's security categorization is used in a future step to select initial security controls for the system. The data owner collaborates with the System Owner and the ISSO to complete the security categorization.

### 5.2.3 TASK C-3: Security Categorization Review and Approval

The system's security categorization from the previous step must be reviewed and approved by the AO, CISO, and SAOP (only for systems with a PIA), or their designated representatives. Delegated representatives must be Federal employees. The ISSO collaborates with the AO, OCISO, Privacy Team, and Data Owner as necessary to have the FIPS 199 security categorization approved. Approval may occur by using GSA's template or collaborating within GSA's GRC tool.

## 5.3 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."

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

### 5.3.1 TASK S-1: Control Selection

The system's baseline determination and overlay selections as described in Task P-4 determines the controls that the system must meet/implement. Any additional requirements/controls necessary for a system's business mission or environment will be coordinated between the system owner and the AO, ISSM, ISSO, and Privacy Team during this control selection task.

**Note: Additional Federal requirements such as CISA Cybersecurity Directives must be included in a system's set of requirements.**

### 5.3.2 TASK S-2: Control Tailoring

After the security controls for a system have been selected in the previous task, tailoring of those controls commences. Tailoring includes:

- Determining common controls the system inherits.
- Assigning values to any parameters identified as being left up to the system for assignment and requiring GSA AO and CISO approval.
- Determining if any compensating or supplemental controls are required to address unique organizational and/or system specific needs. These needs may be based on a risk assessment (either formal or informal), local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.

Justification or rationale for tailoring actions is required, especially where the CISO and AO must approve assignments and if any controls are identified as not applicable to the system or its environment.

Systems must complete a CTW and provide it as an attachment to the SSP. The CTW identifies the GSA defined values for NIST SP 800-53 control assignments and selections. The selected security controls including any controls or enhancements selected above the baseline for the

information system must be documented in the SSP. Similarly, systems must complete a CIS which identifies the control types (common, hybrid, system specific), implementation status (Fully Implemented, Partially Implemented, Planned, etc.), and responsibility (OCISO, GSS/Platform/System) for the system's controls. It will be updated in subsequent steps of the RMF process, including after security control implementation and following security assessment to document the results of the review

Both the SSP and the CTW identify parameter assignments or selections deferred to the SSO or contractor for recommendation and approval by the GSA AO and CISO. The CTW contains columns for identifying the defined values and GSA approval of the values. Table 5-1 contains two examples where a control parameter has been assigned and approved. The agreed upon parameters must be documented in the CTW in order for assessors to know the standard to which they must assess the control.

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

## Table 5-1. Control Statements - Unassigned and Assigned Parameters (Examples)

| Control ID | Control Name | Control Statement | Privacy | Low | Moderate | High | LATO | MiSaaS | Vendor/Contractor Defined Values | GSA Approval of Vendor/Contractor Defined Values |
|---|---|---|---|---|---|---|---|---|---|---|
| CM-02 (03) | Baseline Configuration \| Retention of Previous Configurations | Retain [GSA SSO or Contractor recommended number of previous versions of baseline configurations of the system approved by the GSA CISO and AO] of previous versions of baseline configurations of the system to support rollback. | | | X | X | | | at least two | Approved-[AO] |
| SI-16 | Memory Protection | Implement the following controls to protect the system memory from unauthorized code execution: [GSA SSO or Contractor recommended and GSA CISO and AO approved security safeguards]. | | | X | X | | | Virtual Memory & Paging/Segmentation | Approved-[AO] |

### 5.3.3 TASK S-3: Control Allocation

As part of Tasks P-5: Common Control Identification and P-17: Requirements Allocation the GSA OCISO and the System Owner in collaboration with the OCSIO identified and allocated controls to the system. These controls were further defined in the previous two tasks. Now the System Owner collaborates with the ISSO to identify how controls have been allocated. This task includes verifying the common, hybrid, and system specific designations of controls and the components or elements within the system to which controls are allocated. For example, boundary protection controls may be allocated to components that manage and monitor the system boundary, access control to components that manage access to the system by users and other systems or between components of the systems. The details of control allocation must be documented in the SSP. The System Owner collaborates with the ISSM, ISSO, Privacy Team as necessary, and other System Owners (regarding common/hybrid controls) to complete control allocation.

### 5.3.4 TASK S-4: Documentation of Planned Control Implementations

Systems must complete an SSP using the GSA SSP Template, including the appendices and attachments, as applicable, identified in Appendix D. The SSP provides an overview of the security requirements for the information system and, in this step, describes the controls planned for implementation to provide a level of security appropriate for the information to be transmitted, processed, or stored by the system. Inherited controls must be included. Detailed instructions for completing the SSP are in the GSA SSP Template on the InSite IT Security Forms and Aids web page. The following is an excerpt from those instructions:

- Address each control part (e.g., Part a, Part b).
- Do not just reiterate the control statement. Describe the “who, what, when, where, and how” controls are implemented.
- Address the entire IT stack (e.g., OS, database, network) and all processes that implement a control.
- Describe how GSA-defined parameters are met.
- Ensure parameters deferred to SSO or Contractor recommendation and AO and CISO approval are defined. Describe how those parameters are met.
- If controls are planned versus implemented, a time bound plan must be a part of the implementation details.
- If controls are identified as not applicable, a justification and supporting evidentiary artifacts must be presented.

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

### 5.3.5 TASK S-5: Continuous Monitoring Strategy – System

Systems must adhere to GSA’s continuous monitoring strategy expressed in CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program and CIO-IT Security-08-39: FYxx IT Security Program Management Implementation Plan. These guides define how controls are monitored, how risk is assessed, and how monitoring results are reported. The System Owner, ISSM, ISSO, Privacy Team as necessary, and others collaborate to ensure adherence with GSA’s monitoring guidance for reviewing, and responding, as necessary, to monitoring results. Systems aligning with GSA’s

policies and guidance on continuous monitoring are not required to have a system level continuous monitoring strategy. They do need to document in their SSP (control CA-07) that they follow GSA's continuous monitoring strategy as specified in Section 9.1.6.

### 5.3.6 TASK S-6: Plan Review and Approval

The SSP 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 SSP, including appendices and attachments.

For new systems under development, note that in the Select Step, implementation details may not be fully described since the exact implementation to satisfy control requirements may not be complete. Once completed, the SSP is signed by the System Owner, ISSO, and the ISSM. As applicable the SSP is signed by the Vendor ISSO assigned to the system. The SSP and appendices/attachments as listed in Appendix D will be updated and completed as the security controls are implemented in the RMF Implement Step.

**Note:** Approving the security plan 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 ISB Division must review and approve the Security Architecture before the system's security controls are implemented.

## 5.4 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.

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

### 5.4.1 TASK I-1: Control Implementation

Describe the security and privacy control implementation in the SSP; 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 CSP's CRM. Leveraged SaaS documentation, assessment, and authorizations will be limited to the GSA control baseline authorization target. Customer responsibilities identified by FedRAMP authorized CSPs that are above and beyond the GSA implemented FIPS impact level are recommended but not required to be documented, assessed, and authorized in GSA Leveraged SaaS implementations.

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

The security control implementation descriptions should include planned inputs, expected behaviors, and expected outputs (where appropriate) that are typical for technical controls. The SSP 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 RMF Step 4.

Security controls and, when applicable, privacy controls are documented in Section 13 of the SSP. This section must provide a thorough description of how the NIST SP 800-53 controls for the system are being implemented or planned to be implemented. Detailed instructions for completing the SSP are in the GSA SSP Template, on the InSite IT Security Forms and Aids web page. For each control, descriptions must:

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

Systems leveraging a cloud solution must implement the customer responsibilities identified in the CSP's CRM. Only customer responsibilities associated with the GSA system's final control set (i.e., baseline and applicable overlays) must be addressed.

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 SSP.

### 5.4.2 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 but not limited to infeasibility of the design, new capabilities being made available, patches and upgrades to the system. The SSP must be updated to reflect any changed implementation details, so the SSP always reflects the "as implemented" state of the system. In this manner when assessments, the next RMF step, occurs 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 SSP as necessary.

## 5.5 RMF ASSESS Step

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

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

### 5.5.1 TASK A-1: Assessor Selection

The key to effective assessments is having assessors with the required skills, abilities, and technical knowledge to develop assessment plans, assess controls, and prepare assessment reports. Assessors are selected from GSA's pool of assessors who have the necessary skills, abilities, and knowledge to effectively conduct the assessment.

### 5.5.2 TASK A-2: Assessment Plan

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

**Note: Assessment of additional Federal requirements including, but not limited to, CISA Cybersecurity Directives (i.e., BODs/EDs) must be included in the SAP as appropriate.**

The following security assessment requirements must be defined in the SAP and implemented for GSA systems per their FIPS 199 impact level:

- **All FIPS 199 Moderate and High, and Vendor/Contractor Low** impact systems must be assessed by an independent assessor. The use of an independent assessment team reduces the potential for conflicts of interest when verifying the implementation status and effectiveness of the security controls. Independence, per NIST, is impartiality where the assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the information system or the determination of security control effectiveness.
- **All FIPS 199 impact level** systems must conduct authenticated vulnerability scanning of their servers' operating systems as part of security assessment activities. Configuration/compliance scans shall be to GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as deemed appropriate and approved by the AO and CISO. Where a GSA benchmark exists, configuration scanning must be to the GSA benchmarks. Any scanning tool configured to

support the benchmarks or guidelines identified may be used. Contact OCISO for information on the current tools in use or if there is a question about a specific tool.

- **All FIPS 199 impact level** systems with web servers must conduct an authenticated vulnerability scan for the most current Open Web Application Security Project (OWASP) Top Ten Web Application Security Risks. Any scanning tool configured to support the OWASP Top 10 may be used. Contact OCISO for information on the current tools in use or if there is a question about a specific tool. If necessary, manual testing and/or verification using the most current OWASP Testing Guide and/or CIO-IT Security-07-35: Web Application Security is also acceptable.
- **All FIPS 199 impact level** systems with database servers will have their databases scanned as part of their OS vulnerability scanning.
- **All Internet accessible systems, FIPS 199 High impact level, and High Value Asset (HVA)** systems, are required to complete an independent penetration test (or 'pentest') and provide a Penetration Test Report documenting the results of the exercise as part of the A&A package. These tests will be conducted in accordance with CIO-IT Security-11-51: Conducting Penetration Test Exercises.
- **All HVA** systems are required to undergo a red team exercise as part of their A&A. These exercises will be conducted in accordance with CIO-IT Security-24-130: Conducting Red Team Exercises.
- **FIPS 199 Moderate and High impact level** systems and systems following the Lightweight and MiSaaS authorization processes are required to conduct a static code analysis for all software except closed-source COTS. The tools used must examine the software for common flaws and document the results in a Code Review Report per NIST SP 800-53 Control enhancement SA-11(01).

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

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

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

### 5.5.3 TASK A-3: Control Assessments

Assessors assess the security controls following the SAP and using the NIST 800-53, Revision 5 Test Cases, including any supplemental or updated tests based on the specific system requirements (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. For systems that have a PIA, the Privacy Analyst on behalf of the CPO and SAOP will oversee control assessments for the privacy controls. Systems leveraging cloud solutions must include assessing the implementation of customer responsibilities from a CSP's CRM in the assessment.

### 5.5.4 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 SSP (Control PL-02) can be consolidated into one finding and associated with PL-02. All other findings - Low and above are reported individually in the SAR - this includes:

- NIST 800-53 Control Gaps (i.e., Findings identified as Other than Satisfied with a Planned Action); and
- Vulnerability Scan Findings (i.e., operating system, web application, and configuration scanning) - Independent Security Assessors, on an exception basis, may request to aggregate Low risk scan findings for systems with a large number of such vulnerabilities, into a consolidated finding (by scan type) with a reference to the scan report identifying them. Requests are to be submitted to the GSA ISSM and require ISA Director approval.

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 InSite IT Security Forms and Aids web page. The SAR will be included as part of the authorization package.

The risk assessment should consist of the following steps:

- Identify the list of threats and threat sources to the system. The list should include but not be limited to adversarial outsider and insider threats, accidental user threats, structural threats to its components and facilities, environmental threats to the systems facilities and supporting services.
- Align threat sources, impacts, and events with vulnerabilities.
- Assess each not fully met security control and vulnerability identified during the security assessment. Evaluating the likelihood that threat sources and events will exploit each identified vulnerability.
- Assess the possible impact to the system and GSA if the vulnerability was exploited.
- Make a determination of risk based on the likelihood the threat will exploit the vulnerability, and the resulting impact.
- Evaluate the risks of all identified vulnerabilities to determine an overall level of risk for the system or application.

Assessments must include vulnerability description, assessed risk, and recommendations for correcting the vulnerability. Assessment results for subsystems, if any, should be referenced, as appropriate, in the SAR.

Review and consider ALL risk categories in the process of preparing the final SAR. It is a common mistake to ignore some classes of vulnerabilities or findings since they are incorrectly believed to be "low risk." However, scanning tools generally categorize findings without context. They may identify false positive findings that are not real issues and false negative findings or "low/info risk" findings that may be real issues. A human reader with context and an understanding of how the system works and its environment will understand that some findings

are more important than initially labeled. Moreover, low risk items often enhance the risk of other issues or can successfully be combined to generate higher risk. Once identified, they should be rated appropriately (i.e., no longer Low) in the final SAR. FIPS 199 Low or Moderate systems can possess Critical/Very High and High risk findings the same as FIPS 199 High systems.

The FINAL version of the SAR shall be signed by the Assessor.

### 5.5.5 TASK A-5: Remediation 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 IT Security Forms and Aids web page. The assessors in coordination with the System Owner, ISSO, and other system personnel validate remediated and false positive findings.

### 5.5.6 TASK A-6: Plan of Action and Milestones

A system’s 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).

The system ISSO collaborates with the System Owner, other system personnel, and the ISSM to establish POA&Ms, AORs, and ATO conditions as listed Table 6-1 and described in the sections following the table. Remediation timelines are in Table 6-1.

## Table 6-1. POA&M Requirement Guidance

| POA&M Requirements | | | |
|---|---|---|---|
| **Finding Source** | **Type/Risk Level** | **Remediation Timeline** | **When is a POA&M Required?** |
| **Assessment Findings*** <br>● Government Accountability Office (GAO) audits <br>● Office of the Inspector General (OIG) audits <br>● Financial audits <br>● FISMA Self-Assessments <br>● Security Assessment Reports (SARs) <br>● Penetration Tests | All findings 1:1 finding to POA&M (including Low findings) | Based on risk level (see below) | Upon receiving the final report |
| **Continuous Monitoring Findings** <br>● Configuration scans <br>● Vulnerability scans (OS/Network, etc.) <br>● Web vulnerability scans | KEV | 14 days | Upon exceeding the remediation timeline |
| | Critical (Internet-facing) | 15 days | |
| | Critical/High | 30 days | |
| | Moderate | 90 days | Within 60 days of detection |
| | Low | 180 days | Not applicable** |
| **General Control Gaps** (non-vulnerability findings) | Remediation timelines may be extended (no longer than 1 year) as agreed to between ISSM, System Owner, and ISA Division. All findings shall be added to the POA&M and mitigated within the scheduled remediation timelines or rescheduled timeline with justification in the Milestone Changes column of the POA&M. | | |
| **AOR/ATO Conditions** | | | |
| **Approval:** AO, ISC and ISB Directors <br>**Concurrence:** CISO | KEV, Critical, High | AOR required when associated with a Critical control and remediation timeline exceeded unless tracked as an ATO condition. | |
| **Approval**: AO, ISC and ISB Directors | Moderate | | |
| Not Applicable | Low | AOR/ATO conditions not required (manage in POA&M) | |
| **General Control Gaps** (non-vulnerability findings) | AOR required when associated with a Critical control and remediation timeline exceeded unless tracked as an ATO condition. | | |

*****Do not create POA&Ms for any SAR findings identified as ‘‘Remediated” or “False Positive.” Do not consolidate SAR findings into one POA&M ID.
**Low findings from vulnerability scans are generally informational or false positives and are typically addressed during normal system patching and updates.

#### 5.5.6.1 Findings from Assessments

Every individual finding, regardless of risk level, from the following activities must have its own POA&M (i.e., a 1:1 ratio Finding to POA&M) with remediation timelines as listed in the table above. Do not create POA&Ms for any SAR findings identified as ‘‘Remediated” or “False Positive.” Do not consolidate SAR findings into one POA&M ID.

- Government Accountability Office (GAO) audits
- Office of the Inspector General (OIG) audits
- Financial audits
- FISMA Self-Assessments
- Security Assessment Reports
- Penetration Tests

#### 5.5.6.2 Findings from Continuous Monitoring

POA&Ms are required for all KEV, Critical, and High findings from vulnerability scans and configuration/compliance scans (i.e., continuous monitoring scans) upon detection. Moderate findings are required to have a POA&M within 60 days of detection. Low findings from scans are generally informational or false positives and are typically addressed during normal system patching and updates, and do not require POA&Ms.

#### 5.5.6.3 Exceptions to Remediation Timelines

**Acceptance of Risk Letters (AORs)/ATO Conditions** - Exceptions to remediation timelines for KEV, Critical, High, and Moderate risks require:

- Acceptance of Risk Letters (AORs)–when associated with a Critical control; **OR**
- Must be specifically captured within the ATO letter as a condition with new remediation time(s).

**Note:** AORs for KEV, Critical, and High vulnerabilities require AO, ISC and ISB Directors’ approvals and CISO concurrence. AORs for Moderate vulnerabilities require AO, ISC and ISB Directors’ approvals but not CISO concurrence.

**KEV Catalog Findings** - If vulnerabilities in the KEV Catalog cannot be readily corrected, system owners will be given a 14-day grace period after the CISA-mandated due date or tool detection date (whichever is later) to patch or mitigate the KEV. After this period, the CIO and AO will be notified of the unmitigated risk and a recommendation provided to either; (1) shutdown the system, (2) quarantine the system; allow a POA&M and AOR for no longer than 60 days.

**Control Gap Findings (non-vulnerability findings)** - Remediation timelines may be extended (no longer than 1 year) as agreed to between ISSM, System Owner, and ISA Division. All findings shall be added to the POA&M and mitigated within the scheduled remediation timelines or rescheduled timeline with justification in the Milestone Changes column of the POA&M. An AOR is required when associated with a Critical and the remediation timeline exceeded unless tracked as an ATO condition.

#### 5.5.6.4 Findings from Configuration/Compliance Scans

Findings related to configuration/compliance scans must be covered by a:

- Deviation - The non-compliant setting is covered by an approved deviation.
- POA&M - If the compliance percentage of any asset is below 90% a POA&M must be created for the non-compliant asset. The resultant POA&M will state:

  "Configuration/compliance scans indicate that [Asset] is below 90% compliant."

**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. A GSA POA&M Template is available on the InSite IT Security Forms and Aids web page. 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.

## 5.6 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."

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

### 5.6.1 TASK R-1: Authorization Package

The ISSO assembles the security authorization package. For GSA's Standard A&A process, the security authorization package includes:

- SSP (with all appendices and attachments)
- Security Assessment Report (with all appendices and attachments)
- POA&M
- Certification Letter
- ATO Letter

**Note:** The documents outlined for the Security Authorization Package (above) are required for the GSA Standard A&A Process. Details on the documentation required for other A&A processes GSA uses (and the standard process) are listed in Appendix D.

### 5.6.2 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, SAOP (for systems that have a PIA), and others as necessary to determine if the package provides enough information to establish a credible level of risk.

### 5.6.3 TASK R-3: Risk Response

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

### 5.6.4 TASK R-4: Authorization Decision

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

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

- ISC quality checks and validates the package and prepares a Certification Letter 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.

### 5.6.5 TASK R-5: Authorization Reporting

Authorization decisions are reflected in the system information in GSA's GRC tool with high-level A&A metric data published organization-wide on the GSA EA Analytics & Reporting (GEAR) website. Any risks that need to be raised to the enterprise level are reported through the ERSI and EMB. The CISO is co-chair of the ERSI with members from GSA SSOs and Regional Offices to ensure appropriate risks are raised that may influence GSA's strategy, budget planning, and resource allocation decisions.

## 5.7 RMF MONITOR Step

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

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

### 5.7.1 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.

### 5.7.2 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 Security-01-05: Configuration Management (CM), 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 Process, 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., 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 GSA ISCM Enterprise Management Tools. GSA's tool stack facilitates the ongoing assessments of GSA information systems by performing vulnerability scans and checking the configuration settings of systems against GSA required hardening benchmarks.

### 5.7.3 TASK M-3: Ongoing Risk Response

ISSOs, System Owners, and system, network, and database administrators, will coordinate and perform remediation actions based upon the results of ongoing monitoring activities, assessment of risk, and outstanding items in the system's POA&M. CIO-IT Security-01-05: Configuration Management (CM) outlines the implementation of a CM process designed to lower the potential risk to a network by requiring regular "patching" or repairing of known vulnerabilities. CIO-IT Security-01-05 addresses the required steps for implementing changes; Identifying Changes, Evaluating Change Requests, Decision Implementation, and Implementing Approved Change Requests. Per CIO-IT Security-18-91: Risk Management Strategy (RMS), risk mitigation shall be the appropriate risk response for all Critical/Very High and High risk vulnerabilities that can be exploited from the Internet and cannot be accepted, avoided, shared, or transferred. Risks from identified vulnerabilities must be remediated based on the timelines specified in NIST SP 800-53 control RA-05 in Section 9.3.4. No standard remediation timeline is established for Low/Very Low vulnerabilities; they are to be addressed in the normal course of patching or configuration management of a system. Risk mitigation strategies may include business process improvements, applying timely patches, configuring systems securely, performing secure application code development, and implementing architecture and design modifications as necessary. Risk mitigation measures will be employed based on prioritization. Some of the risk prioritization assessment criteria may include the probability of vulnerability exploitation, material business impact if vulnerability is successfully exploited, compliance requirements, cost and business impact of remediation activities and controls.

Specific categories of risks as described below may be accepted.

**Acceptance of Risk (AOR) Letters.** AOR letters are intended for circumstances where the System Owner has limited or no control over the remediation of an identified risk. Examples of such circumstances include:

- Commercial off-the-shelf (COTS) product update timelines
- Compatibility issues between components
- Contractual issues that prohibit remediation;
- Embedded software dependencies; and
- KEV, Critical/Very High, High, and Moderate risk vulnerabilities associated with Critical controls and the remediation timeline is exceeded, unless tracked as an ATO condition.

**Note:** Due to the significant risk the KEVs pose to the federal government, AORs will only be authorized with CISO and AO approval for no longer than 60 days. AOR requests should only be submitted based on an operational risk outweighing the security risk.

AORs are not intended for:

- Delayed or ineffective flaw remediation processes (e.g., patching, addressing known vulnerabilities);
- Insufficient out-year System Development Life Cycle planning (for legacy components);
- System Owner preferences not supported by OCISO guidance and policies;

AOR requests must include mitigating factors, compensating controls, and any other action(s) taken to reduce the risk to the system and its data, and a justification for why the vulnerability cannot be resolved. The maximum duration of an AOR letter is one year. However, the duration should be only for as long as is necessary to remediate the vulnerabilities/findings for which the letter is being prepared (e.g., if remediation will only take 3 months the duration should be 3 months). If remediation cannot be completed within the duration of the AOR letter, a new AOR letter must be prepared. The new AOR letter must include new/current details as to why the vulnerabilities/findings were not able to be remediated and the risk description revised, as necessary. Because the resolution exceeded the original AOR letter duration, the ISC Director must discuss the rationale for the new AOR letter with the CISO. Evidence of this discussion (date, etc. must be documented in the AOR letter).

Based on the criteria above, AOR letters are approved as indicated below:

- Moderate risk AOR letters require AO, ISC Director, and ISB Director approval, but not CISO concurrence.
- KEV, Critical, and High risk AOR letters require AO, ISC Director, and ISB Director approval, and CISO concurrence.

**AOR Letter Processing.** AOR letters are processed in the following manner:

1. The System Owner/Custodian, Component System Owner (if applicable), ISSO, and ISSM determine the need for an AOR letter.
2. The ISSO in conjunction with the ISSM prepares the AOR letter, including creation of an AOR ID# as specified below. NN is a sequential number of the AOR, YYYY is the current Fiscal Year, the brackets are not part of the AOR ID#.

   AOR-NN-[System Acronym]-YYYY Example: AOR-02-EIO-2026

3. The ISSM coordinates with the ISC Director to determine if a review discussion is appropriate with stakeholders and/or the CISO. If a review discussion is required, they jointly schedule the discussion and update the letter, if necessary.
4. Prior to AOR approval processing, the System Owner must brief the Authorizing Official (AO) on risk acceptance.
5. The ISSM submits the AOR letter to:
   a. ISB and ISC Directors and the AO for approval of any Moderate risk AORs.
   b. ISB and ISC Directors and the AO for approval and CISO for concurrence for any KEV, Critical and High risk AORs.

6. Approved AOR letters are part of the permanent A&A files maintained by the ISSO and ISSM. AOR letters must be uploaded into the corresponding FISMA system's A&A Repository in GSA's GRC tool, and an email sent to ispcompliance@gsa.gov indicating an AOR letter has been uploaded.
7. The ISSO is responsible for monitoring POA&Ms and AOR letters. When an AOR is within 30 days of expiring:
   a. If any POA&Ms listed in the AOR letter will not be resolved, a new AOR letter is required as described above.
   b. If all POA&Ms have been, or will be resolved prior to AOR letter expiration, then after all POA&Ms have been resolved the AOR letter is noted as completed and archived as a historical record of the system's A&A status.

AORs are reviewed on a monthly basis by the ISA Division. Any issues or pending deadlines are coordinated with the appropriate personnel

### 5.7.4 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.

- SSP (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;
- Changes identified as part of a system's CM Plan;
- For systems in the GSA OA Program, performance metrics established as part of ongoing authorization per CIO-IT Security-12-66.

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 SSP will be updated to reflect any changes.

Updates to authorization packages are also required when Federal or GSA guidance changes or implementations the system relies on change. Systems must update their A&A packages when the following occur:

- When a FedRAMP CRM used by a system is updated (e.g., with new features or revised requirements), the system must update its CRM control implementations and complete an assessment within 12 months of the CRM's release date.
- When an updated GSA Control Tailoring Workbook (CTW) is released (e.g., with changes to control parameters or new requirements), systems must update their System SSP control implementations within 12 months. An assessment or delta assessment for these updates is only required if specifically communicated by OCISO leadership.
- When a Common Control provider releases an update (e.g., with changes to control parameters or new requirements), systems must update their SSP control

implementations within 12 months of the providers release date. An assessment or delta assessment for these updates is only required if specifically communicated by OCISO leadership.

### 5.7.5 TASK M-5: Security and Privacy Reporting

The System Owner and ISSO will report the security and privacy status of the information system (including the effectiveness of security and privacy controls employed within and inherited by the system) to the AO, the SAOP, for systems that have a PIA, and other appropriate organizational officials on an ongoing basis. GSA's vulnerability management program, the POA&M management process, privacy program, and any required reporting processes/capabilities (e.g., FISMA, OA, CDM) will be used to provide security and privacy status reporting. AOs and other personnel with security and privacy related responsibilities will leverage these resources to keep apprised of the risk levels associated with GSA's system(s).

### 5.7.6 TASK M-6: Ongoing Authorization

GSA's OA Program as described in CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program relies on GSA's continuous monitoring strategy. That strategy leverages both manual and automated processes to monitor a system's security and privacy controls. The objective of the strategy is to ensure all key information security and privacy controls are periodically assessed for effectiveness. It leverages GSA's deployment of CDM and other GSA ISCM Enterprise Management Tools to monitor the security of GSA's systems. CIO-IT Security-12-66 provides more details on how GSA continuously monitors vulnerabilities, threats, and actions taken to reduce, mitigate, or eliminate them. Key components of GSA's strategy are regular vulnerability scanning activities and security configuration checks, the requirement to maintain A&A documents in an "as-is" state, management and review of POA&Ms, and ISSO Checklists within GSA's GRC tool.

To enter the OA Program systems must meet prerequisites defined in CIO-IT Security-12-66 and successfully complete the onboarding process which includes completion of a checklist verifying the security status of the system, review of GSA's OA and Critical controls, review of system artifacts, verifying that GSA security tools are in place and monitoring the system. The GSA OA Team coordinates with System Owner, ISSM, and ISSO during the onboarding process and semi-annual performance reviews for systems in the OA Program.

### 5.7.7 TASK M-7: System Disposal

System Owners and ISSOs must manage systems from inception through disposal in accordance with GSA Order CIO 2101.3, "GSA Integrated Information Technology Management," and the GSA Solutions Life Cycle Handbook. In support of system disposal system owners will document the transfer and/or disposal of GSA IT Systems using GSA's Transfer and Disposal Notification Templates and in accordance with the provisions outlined within CIO 2100.1, "GSA Information Technology (IT) Security Policy."

## 5.8 A&A Guidance for Significant Changes

Significant changes are identified by using the decision tree in Appendix E to determine if a change is significant or not significant. Contact the OCISO at ispcompliance@gsa.gov if there are questions about using the decision tree.

## 5.9 A&A Guidance for Expiring Authorizations

ISSOs, ISSMs, and the ISC Director can track the expiration dates of ATOs using GSA's GRC tool. Renewals of ATOs are initiated by the AOs, ISSMs, and ISSOs. The following extracts from CIO 2100-GSA Cybersecurity Handbook contain further guidance:

Section 5. Policy for Identify

Subsection 5.1, Asset Management

Part g. Assessment and Authorization (A&A)

(4) Extension of a system's current ATO for a period not to exceed one year (365 days) may only be requested under one of the following conditions. The system must continue to maintain its complete set of A&A documentation as listed in GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk. All actions to satisfy the following conditions below must be completed within the extension period (i.e., no longer than 12 months).

(a) Transitioning to ongoing authorization;
(b) Planning for disposal;
(c) Consolidating into another system for its ATO. The scope of consolidation shall be approved by the OCISO prior to submitting the ATO extension request;
(d) Transitioning into a cloud environment for its ATO. The scope of the transition into the cloud environment shall be approved by the OCISO prior to submitting the ATO extension request;
(e) Re-competing the system's contract;
(f) Completing the upgrade/replacement of major infrastructure components;
(g) Completing the system's security assessment has been delayed due to contract issues; or
(h) Complying with Critical controls as listed in CIO-IT Security-06-30.

(5) An information system undergoing a three-year re-authorization having outstanding High or Critical/Very High vulnerabilities identified during its security assessment, may request a one-time extension for a period not to exceed thirty (30) days from the date of the ATO expiration to allow mitigation of the High and Critical/Very High vulnerabilities. No more than two extensions may be granted under this condition.

**Note:** The CISO may also grant extensions on a case-by-case basis due to extenuating circumstances.

Questions concerning the security authorization process, significant changes, or expiring ATOs can be directed to the designated ISSM.

# 6 Protecting CUI in Nonfederal Systems and Organizations

CIO-IT Security-21-112: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations Process, defines the processes and procedures that will be used to ensure nonfederal systems protect CUI in accordance with the requirements of NIST SP 800-171, Revision 3, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." The requirements identified in both documents are applicable under the following conditions:

- CUI is resident in a nonfederal system and organization;
- the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency;[2] and
- there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.[3]

The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or provide security protection for such components.

# 7 Assessing Building Monitoring and Control (BMC) Solutions

CIO-IT Security-16-76: Building Monitoring and Control (BMC) Systems Security Assessment Process, defines the procedures for assessing BMC solutions submitted to the GSA OCISO by the Public Building-Information Technology (PB-ITS) Building Technology Services (BTS) Division. BMC devices are a subset of Operational Technology (OT) and include Internet of Things (IoT) devices used in building management. All IoT devices, as defined in GSA Order CIO 2100.1, GSA IT Security Policy, must adhere to the requirements in NIST SP 800-213, “IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements" or receive a waiver from GSA under one of the conditions of Public Law 116-127, “Internet of Things Cybersecurity Improvement Act of 2020.”

# 8 Independent Assessment of Enterprise-wide Common and Hybrid Controls

CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC) fulfills the requirement for a security program per NIST SP 800-53, Control PM-01, Information Security Program Plan. NIST SP 800-37, requires that common controls be assessed and authorized. The controls in the CCC (both common and the common portion of hybrid controls) are assessed at least every three years or when applicable Federal or GSA requirements have been updated. The CISO and CPO authorize the controls within the CCC when it is signed by them.

# 9 GSA Implementation of CA, PL, and RA Controls

NIST SP 800-53 defines controls related to the security authorization process that GSA is required to implement based on an information system’s security categorization. The Assessment, Authorization, and Monitoring (CA), Planning (PL), and Risk Assessment (RA) control family implementations are addressed in this guide. Only those controls applicable at any FIPS 199 Level in accordance with NIST SP 800-53B are included in this section.

For readers’ ease of use, “mini tables” (see table below) that contain control/enhancement designation and applicability information is provided at the end of control statements for each

[2] Nonfederal organizations that collect or maintain information *on behalf of* a federal agency or that use or operate a system *on behalf of* an agency, must comply with the requirements in the Federal Information Security Modernization Act (FISMA), including the requirements in [FIPS 200] and the security controls in [SP 800-53] (See [44 USC 3554] (a)(1)(A)).

[3] The requirements in NIST SP 800-171 can be used to comply with the [FISMA] requirement for senior agency officials to provide information security for the information that supports the operations and assets under their control, including CUI that is resident in nonfederal systems and organizations (See [44 USC 3554] (a)(1)(A) and (a)(2)).

control. The tables allow readers to see if a control/enhancement is applicable at their system's FIPS Level/A&A process and if it is common (C), Hybrid (H), or system specific (S).

**Example**

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| Control ID | ✓ | ✓ | ✓ | | | C | H |

## 9.1 Assessment, Authorization, and Monitoring (CA)

### 9.1.1 CA-01 Policy and Procedures

**Control:**

a. Develop, document, and disseminate to [personnel with IT security responsibilities as defined in GSA CIO Order 2100.1]:
   1. [Organization-level] assessment, authorization, and monitoring policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

b. Designate an [CISO] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:
   1. Policy [review annually and update as necessary] and following [changes to Federal or GSA policies, requirements, or guidance]; and
   2. Procedures [at least every three (3) years] and following [changes to Federal or GSA policies, requirements, or guidance].

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| CA-01 | ✓ | ✓ | ✓ | | | C | C |

**GSA Implementation Guidance:**

The GSA security assessment and authorization policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding assessing and authorizing systems for GSA. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency Directives Library website.

Security assessment and authorization procedures are documented in this guide. Additional security and assessment guides for specific types of systems have been developed and are referenced in this guide. The procedures in these guides facilitate the security assessment and authorization of all GSA systems. The guides are disseminated GSA-wide via GSA's InSite centralized agency IT Security Procedural Guides website.

The GSA CISO is responsible for managing the development, documentation, and dissemination of all IT security policies procedural guides.

The GSA OCISO is responsible for reviewing CIO 2100.1 annually and updating it as necessary, and following changes to Federal or GSA policies, requirements, or guidance.

The GSA OCISO is responsible for reviewing and updating CIO-IT Security 06-30 at least every three (3) years and following changes to Federal or GSA policies, requirements, or guidance.

**Contractor System Considerations:** Vendors/contractors must adhere to GSA's policy and guide regarding the security assessment and authorization of GSA systems.

### 9.1.2 CA-02 Control Assessments

**Control:**

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted
b. Develop a control assessment plan that describes the scope of the assessment including:
   1. Controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;
c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
d. Assess the controls in the system and its environment of operation [annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
e. Produce a control assessment report that document the results of the assessment; and
f. Provide the results of the control assessment to [personnel with system security responsibilities as identified in CIO 2100.1 and CIO-IT Security 06-30].

**Control Enhancements:**

(01) Control Assessments | Independent Assessors – Employ independent assessors or assessment teams to conduct control assessments.
**Note:** Assessors are independent if they do not: (i) have a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are assessing; or (iv) place themselves in positions of advocacy for the organizations acquiring their services.

(02) Control Assessments | Specialized Assessments – Include as part of control assessments [annual], [announced], [penetration testing].

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| CA-02 | ✓ | ✓ | ✓ | | ✓ | C | H |
| CA-02(01) | ✓* | ✓ | ✓ | | | C | C |
| CA-02(02) | | | ✓ | | | C | S |

*only for external vendor/contractor systems

**GSA Implementation Guidance:**

GSA requires a security control assessment to be performed as defined in Section 5.5 of CIO-IT-Security 06-30. The tasks in that section include the selection of the appropriate assessors, the development of an assessment plan identifying the controls to be assessed, the procedures to be used, the team, environment, and roles and responsibilities. The plan is required to be approved before the assessment can begin. The execution of the assessment plan and the preparation of the assessment report is described, including the report being part of the A&A package that is provided to the ISSM, CISO, System Owner, and AO. Assessments for GSA's A&A processes are summarized in Section 4 which includes a document reference where assessment processes for a specific A&A process can be found.

As per CA-02(01), GSA FIPS 199 Moderate and High Impact Systems must be assessed by an independent assessor. All FIPS 199 Low external vendor/contractor systems must be assessed by an independent assessor. The use of an independent assessment team reduces the potential for partiality or conflicts of interest when verifying the implementation status and effectiveness of the security controls.

As per CA-02(02), GSA FIPS 199 High Impact Systems must be assessed annually via announced penetration tests. Penetration testing provides a more thorough analysis of the implementation effectiveness of security controls associated with an information system.

**Contractor System Considerations:** Vendors/contractors must adhere to GSA's policy and the controls regarding the security assessment of GSA systems.

### 9.1.3 CA-03 Information Exchange

**Control:**

a. Approve and manage the exchange of information between the system and other systems using [IEAs/ISAs/MOAs as applicable per CIO-IT Security-24-125: Managing Information Exchange Agreements and documented in the system's SSP Section 11-System Interconnections (Table 11-1 and 11-2)];
b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
c. Review and update the agreements [as specified in each IEA/ISA/MOA].

**Control Enhancements:**

(06) Information Exchange | Transfer Authorizations – Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| CA-03 | ✓ | ✓ | ✓ | | | S | S |
| CA-03(06) | | | ✓ | | | S | S |

**GSA Implementation Guidance:**

The focus of this control is to ensure that information exchanges to any other information system outside of the system's authorization boundary have been approved by the AO, identified, and documented within the SSP, and monitored on an ongoing basis. CIO-IT Security 24-125: Managing Information Exchanges defines how exchanging information between GSA systems and between GSA and external systems must be securely managed, any types of agreements required, and the approval authority for the information exchanges.

As per CA-03(06), GSA FIPS 199 High Impact Systems must ensure the appropriate authorizations (i.e., write permissions or privileges) between the individuals or systems transferring data between the interconnecting systems have been verified prior to accepting such data.

**Contractor System Considerations:** Vendors/contractors must adhere to GSA policies and guides and the control requirements regarding information exchanges, the documentation/agreements necessary and the approval of the exchange/connection.

### 9.1.4 CA-05 Plan of Action and Milestones

**Control:**

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
b. Update existing plan of action and milestones [at least quarterly] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| CA-05 | ✓ | ✓ | ✓ | | | S | S |

**GSA Implementation Guidance:**
The focus of this control is to ensure that all information systems have developed a POA&M in accordance with CIO-IT 09-44: Plan of Action and Milestones (POA&M) which details the POA&M processes and procedures for meeting the requirements of this control.

On a quarterly basis, POA&Ms will be reviewed by the OCISO ISA Division in order to monitor agency-wide remediation efforts as required by OMB policy. Updates to POA&Ms should be performed by the ISSO as milestones or actions occur throughout the year. POA&Ms are located on individual system POA&M Share Drives and are maintained by the system ISSO or ISSM. The POA&M Shared Drives serve as the primary location for managing and communicating GSA's system and program POA&Ms, and are accessible via GSA's network, or via VPN.

New systems that are currently undergoing a security authorization process or that have not been included in the GSA FISMA inventory must use the POA&M Template available on the POA&M Guidance Shared Drive or contact ispcompliance@gsa.gov to have a shared drive and POA&M created.

**Contractor System Considerations:** Contractor systems must provide POA&Ms through their ISSO(s) as contractors will not have access to the POA&M Shared Drives. ISSOs supporting these systems must facilitate POA&M updates by sending the current version of the system POA&M together with the OCISO guidance to the contractor representative(s). **Note: POA&Ms and GSA's guidance are CUI and must be protected and transmitted IAW GSA CUI guidance.** Upon receipt of the POA&M from the contractor, ISSOs shall review the POA&M to ensure it is updated and includes required vulnerabilities before updating the POA&M on the GSA POA&M Shared Drives.

### 9.1.5 CA-06 Authorization

**Control:**

a. Assign a senior official as the authorizing official for the system;
b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;
c. Ensure that the authorizing official for the system, before commencing operations:
   1. Accepts the use of common controls inherited by the system; and
   2. Authorizes the system to operate;
d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
e. Update the authorizations [as specified in CIO-IT Security-06-30 and GSA's other Assessment and Authorization processes identified therein].

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| CA-06 | ✓ | ✓ | ✓ | | | H | H |

**GSA Implementation Guidance:**
The OCISO issues AO Designation Letters identifying the authorizing official for all GSA information systems.

If a platform or system providing controls for other systems is authorized to operate, any common controls it is providing are authorized by the assigned AO.

CIO 2100.1, “GSA Information Technology (IT) Security Policy,” and CIO-IT-Security 06-30: Managing Enterprise Cybersecurity Risk require AOs to review and approve security safeguards of information systems and issue ATO approvals for each information system, application, or set of common controls under their purview based on the acceptability of the implementation of security safeguards in place (risk-management approach).

CIO 2100.1 and CIO-IT Security 06-30 state that final authority to operate or not operate an information system, application, or a set of common controls rests with the AO.

CIO 2100.1 and CIO-IT Security-06-30 require authorizations to be updated in accordance with the timelines defined in CIO-IT Security-06-30 and GSA’s other A&A process guides. As specified in CIO-IT Security-06-30, authorizations are updated at least every three years or upon significant changes. Systems in ongoing authorization undergo biannual performance metric monitoring which fulfills the update requirement.

**Contractor System Considerations:** AOs, System Owners, ISSOs, and ISSMs are responsible for coordinating the update of Vendor/Contractor security authorization packages and submitting them to the OCISO in accordance with the timelines defined in CIO-IT Security-06-30 and CIO-IT Security-19-101: External Information System Monitoring.

### 9.1.6 CA-07 Continuous Monitoring

**Control:**
Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: [as specified in Section 3 of CIO-IT Security-08-39: Management Implementation Plan and CIO-IT Security-12-66: ISCM Strategy and OA Program];
b. Establishing [frequencies as specified in Section 3 of CIO-IT Security-08-39: Management Implementation Plan and CIO-IT Security-12-66: ISCM Strategy and OA Program] for monitoring and [frequencies as specified in Section 3 of CIO-IT Security-08-39, Management Implementation Plan and CIO-IT Security-12-66: ISCM Strategy and OA Program] for assessment of control effectiveness;
c. Ongoing control assessments in accordance with the continuous monitoring strategy;
d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
e. Correlation and analysis of information generated by control assessments and monitoring;
f. Response actions to address results of the analysis of control assessment and monitoring information; and
g. Reporting the security and privacy status of the system to [CISO, AOs, System Owners, ISSMs, ISSOs, Custodians] [as specified in CIO-IT Security-08-39: Management Implementation Plan and CIO-IT Security-12-66: ISCM Strategy and OA Program].

**Control Enhancements:**

(01) Continuous Monitoring | Independent Assessment – Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

**NOTE:** Independence is waived for all annual testing (i.e., testing can be internally performed).

(04) Continuous Monitoring | Risk Monitoring – Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:
(a) Effectiveness monitoring;
(b) Compliance monitoring; and
(c) Change monitoring.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| CA-07 | ✓ | ✓ | ✓ | ✓ | ✓ | H | H |
| CA-07(01) | | ✓ | ✓ | | | C | C |
| CA-07(04) | ✓ | ✓ | ✓ | | | C | C |

**GSA Implementation Guidance:**

Systems aligning with GSA's policies and guidance on continuous monitoring do not have to have a system level continuous monitoring strategy. They do need to document in their SSP that they follow GSA's continuous monitoring strategy as specified below and identified in CIO-IT Security-Privacy-18-90: Common Control Catalog.

The GSA OCISO developed CIO-IT Security-12-66: Information Security Continuous Monitoring Strategy (ISCM) & Ongoing Authorization (OA) Program and has established system-level metric monitoring and control assessment requirements, as defined by CIO-IT Security-08-39: FYxx IT Security Program Management Implementation Plan and CIO-IT Security-12-66.

Systems' ongoing control assessments are performed based on GSA's ATO processes defined by CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk and CIO-IT Security-12-66

for systems accepted into the OA Program. Additionally, the OCISO requires systems to complete an annual FISMA Self-Assessment unless they have completed a full assessment in the current FY.

The GSA OCISO performs ongoing monitoring of system and organization-defined metrics using automated enterprise management tools and manual processes defined by:

- CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk
- CIO-IT Security-08-39: FYxx IT Security Program Management Implementation Plan
- CIO-IT Security-09-44: Plan of Action and Milestones (POA&M)
- CIO-IT Security-17-80: Vulnerability Management Process
- CIO-IT Security-18-91: Risk Management Strategy (RMS)
- CIO-IT Security-19-101: External Information System Monitoring.

System Owners, ISSOs, and ISSMs are responsible for monitoring and adhering to assigned system level metrics in accordance with GSA IT Security Policies and procedures.

System-assigned ISSOs and ISSMs record and manage the mitigation and remediation of identified weaknesses and deficiencies that are not associated with accepted risks in organizational information systems' POA&M per CIO-IT Security-09-44. System-assigned ISSOs and ISSMs continuously perform system-level correlation and analysis of assessment results and system risk monitoring activities by performing POA&M management in coordination with System Owners and system custodians.

The GSA OCISO performs POA&M reviews upon completion of an A&A and quarterly thereafter. System level quarterly POA&M Review Reports are generated by the OCSIO and are provided to ISSOs for quality reviews and process improvement activities. AO/CISO Quarterly Management Reports are generated by the OCISO to provide an agency view of Cybersecurity and Risk Management priorities to each AO. Each is generated per the AO's managed system portfolio includes ATO statuses, AOR and ATO Condition remediation status, and additional applicable risk considerations.

The GSA OCISO has established and defined system-level response action requirements within:

- CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk
- CIO-IT Security-09-44: Plan of Action and Milestones
- CIO-IT Security-17-80: Vulnerability Management Process

The GSA OCISO has established and defined methods for reporting system-level security and privacy status within CIO-IT Security-08-39 and CIO-IT Security-12-66. The OCISO conducts quarterly AO/CISO briefings during which systems' cyber hygiene and operational statuses are reported to the AOs.

System Owners, ISSOs, ISSMs, and system custodians are responsible for reporting system-level security and privacy statuses per predefined reporting frequencies and mechanisms (e.g., ISSO Checklists, POA&Ms, and ad hoc data calls).

Per CA-07(01), the ISA Division performs operational oversight of the agency's ISCM strategy and OA Program. ISA performs assessment activities of the information systems accepted into the OA Program, per the program's monitoring and reporting requirements and with impartiality.

Per CA-07(04), the OCISO has established CIO-IT Security-12-66: Information Security Continuous Monitoring Strategy (ISCM) & Ongoing Authorization (OA) Program that includes

effective compliance and risk monitoring policies and procedures defined by CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk. The guidance establishes the agency's assessment, authorization, and monitoring requirements for each managed GSA information system. The procedural requirements define the continuous monitoring of system controls and relevant documents, or records created by the agency in performing lifecycle management activities; e.g., SAPs, POA&Ms, SSPs, and SARs.

**Contractor System Considerations:** System Owners, ISSOs, and ISSMs are responsible for the continuous monitoring of system level metrics, assessments, response actions, reporting, and risk monitoring in accordance with the guides identified above for vendor/contractor systems.

### 9.1.7 CA-08 Penetration Testing

**Control:**
Conduct penetration testing [during A&A efforts and annually thereafter] on [all Internet accessible, FIPS 199 High impact, and High Value Asset (HVA) information systems].

**Control Enhancements:**

(01) Penetration Testing | Independent Penetration Testing Agent or Team - Employ an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

**NOTE:** Independence is waived for all annual testing (i.e., testing can be internally performed).

(02) Penetration Testing | Red Team Exercises - Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [as defined in CIO-IT Security-24-130: Conducting Red Team Exercises].

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| CA-08 | ✓* | ✓* | ✓ | ✓* | ✓ | H | S |
| CA-08(01) | ✓* | ✓* | ✓ | | ✓ | C | S |
| CA-08(02) | ✓** | ✓** | ✓** | | ✓** | C | S |

*if Internet accessible/HVA

**if HVA

**GSA Implementation Guidance:**
For systems in scope per the defined parameter, the GSA OCISO Penetration Testing team can provide penetration testing in support of GSA systems' A&A and annual penetration testing requirements as described in CIO-IT Security-11-51: Conducting Penetration Test Exercises. If the GSA OCISO Pen Testing team is used, coordination between the system team and the Penetration testing team is required to coordinate the effort. If another entity performs the penetration testing the processes and procedures in CIO-IT Security-11-51 still must be followed.

Per CA-08(01), the GSA OCISO Penetration Testing team performs penetration testing activities on behalf of GSA as an independent testing agent. The GSA OCISO Penetration Testing team is free from any perceived or actual conflicts of interest with respect to the

development, operation, or management of the systems that are the targets of the penetration testing activities performed by the team. Independence is waived for all annual testing (i.e., testing can be internally performed).

Per CA-08(02), All GSA HVAs are required to undergo a red team exercise as part of their A&A and annually thereafter.

**Contractor System Considerations:** If the GSA OCISO Penetration Testing team performs the penetration test, the System Owner, ISSO, and ISSM must coordinate with the penetration testing team to schedule their services. If an external penetration testing vendor performs the penetration test, the external penetration testing vendor must complete the minimum requirements set forth in CIO-IT Security-11-51. As identified above, the OCISO Penetration Testing team is independent; if penetration testing is performed by an external vendor, independence must be documented and accepted by the OCISO. Independence is waived for all annual testing (i.e., testing can be internally performed).

All Vendor/Contractor systems GSA designates as an HVA are required to undergo an annual Red Team exercise. A Red Team Exercise Report must be submitted to GSA.

### 9.1.8 CA-09 Internal System Connections

**Control:**

a. Authorize internal connections of [other GSA components using a secure methodology providing security commensurate with the acceptable level of risk as defined in the SSP and limits access to the information needed by the connected component] to the system;
b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;
c. Terminate internal system connections after [15 minutes of inactivity for non-persistent connections]; and
d. Review [annually (or as the SSP is reviewed and updated)] the continued need for each internal connection.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| CA-09 | ✓ | ✓ | ✓ | | | S | S |

**GSA Implementation Guidance:**
If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the SSP and that limits access only to the information needed by the other system. GSA-IT Security-24-125: Managing Information Exchanges defines how information between GSA systems and between GSA and external systems must be secured and agreements approved when necessary.

**Contractor System Considerations:** Vendors/contractors must adhere to GSA policies and guides and the control requirements regarding internal system connections.

## 9.2 Planning (PL)

### 9.2.1 PL-01 Policy and Procedures

**Control:**

a. Develop, document, and disseminate to [personnel with IT security responsibilities as defined in GSA CIO Order 2100.1]:
   1. [Organization-level] planning policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;
b. Designate an [CISO] to manage the development, documentation, and dissemination of the planning policy and procedures;
c. Review and update the current planning:
   1. Policy [review annually and update as necessary] and following [changes to Federal or GSA policies, requirements, or guidance]; and
   2. Procedures [at least every three (3) years] and following [changes to Federal or GSA policies, requirements, or guidance].

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| PL-01 | ✓ | ✓ | ✓ | | | C | H |

**GSA Implementation Guidance:**
The GSA security planning policy is defined in GSA Order CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding the security planning for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency Directives Library website.

Planning procedures are documented in this guide. The procedures facilitate the implementation of the security planning policy and associated controls. The guide is disseminated GSA-wide via GSA's InSite centralized agency IT Security Procedural Guides website.

The GSA CISO is responsible for managing the development, documentation, and dissemination of all GSA IT security policies procedural guides.

The GSA OCISO is responsible for reviewing 2100.1 annually and updating it as necessary, and following changes to Federal or GSA policies, requirements, or guidance.

The GSA OCISO is responsible for reviewing and updating CIO-IT Security-06-30 and all procedural guides at least every three (3) years and following changes to Federal or GSA policies, requirements, or guidance.

**Contractor System Considerations:** Vendors/contractors may defer to the GSA policy and guide or implement their own security planning policies and procedures which comply with GSA's requirements with the approval of the GSA CISO and AO.

### 9.2.2 PL-02 System Security and Privacy Plans

**Control:**
a. Develop security and privacy plans for the system that:

1. Are consistent with the organization's enterprise architecture;
2. Explicitly define the constituent system components;
3. Describe the operational context of the system in terms of mission and business processes;
4. Identify the individuals that fulfill system roles and responsibilities;
5. Identify the information types processed, stored, and transmitted by the system;
6. Provide the security categorization of the system, including supporting rationale;
7. Describe any specific threats to the system that are of concern to the organization;
8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
10. Provide an overview of the security and privacy requirements for the system;
11. Identify any relevant control baselines or overlays, if applicable;
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
13. Include risk determinations for security and privacy architecture and design decisions;
14. Include security- and privacy-related activities affecting the system that require planning and coordination with [personnel with IT security responsibilities for the system as defined in GSA CIO Order 2100.1 and the GSA Privacy Office (for systems with Privacy Act data)]; and
15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to [personnel with IT security responsibilities for the system as defined in GSA CIO Order 2100.1];
c. Review the plans [annually];
d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
e. Protect the plans from unauthorized disclosure and modification.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| PL-02 | ✓ | ✓ | ✓ | ✓ | ✓ | S | S |

**GSA Implementation Guidance:**
The focus of this control is to ensure that an SSP has been developed for the information system that documents the security requirements for the information system, and the implementation status of the security controls that have been assigned to the system as per FIPS 199 impact analysis. All GSA information systems must develop an SSP when required by GSA's A&A processes described in this guide and GSA's other A&A. GSA's SSP templates, including associated appendices and attachments, must be used to ensure the control requirements are addressed. Detailed guidance is available through Section 5 of this guide and in the other A&A guides GSA publishes.

SSPs are distributed to personnel with IT security responsibilities for the system by the system team and ISSO and are required to be uploaded to GSA's GRC tool. SSPs are required to be reviewed and updated at least annually to address changes to the system, its environment of operation, control monitoring and assessments. SSP distribution is restricted personnel with IT

security responsibilities for the system as defined in GSA CIO Order 2100.1 to protect against unauthorized disclosure and modification.

**Contractor System Considerations:** Vendors/contractors must adhere to GSA policies and guides and the control requirements regarding SSP development, distribution, review, updates, and protection.

### 9.2.3 PL-04 Rules of Behavior

**Control:**

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;
b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;
c. Review and update the rules of behavior [at least annually]; and
d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [annually or when the rules are revised or updated].

**Control Enhancements:**

(01) Rules of Behavior | Social Media and External Site/Application Usage Restrictions - Include in the rules of behavior, restrictions on:
   a. Use of social media, social networking sites, and external sites/applications;
   b. Posting organizational information on public websites; and
   c. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| PL-04 | ✓ | ✓ | ✓ | | | H | H |
| PL-04(01) | ✓ | ✓ | ✓ | | | C | H |

**GSA Implementation Guidance:**
GSA has developed GSA Order CIO 2104.1, “GSA Information Technology (IT) General Rules of Behavior.” The rules describe a user’s responsibilities and expected behavior when using GSA information systems, including use of social media and external sites/applications, posting organizational information on public websites, and using organizational identifiers or authentication secrets when creating accounts on external sites/applications. All GSA IT users must sign the GSA IT General Rules of Behavior for General Users within 90 days of their entry on duty (EoD). GSA does not require the rules be signed before accessing an information system. GSA OCISO reviews and updates the GSA IT Rules of Behavior for General Users annually. All GSA IT users are required to re-sign the GSA IT Rules of Behavior for General Users annually or when the rules are revised or updated as part of GSA’s annual IT Security and Privacy Awareness training.

As per PL-04 (01), CIO 2104.1 includes restrictions on the use of social media, social networking, and external sites; guidance on posting organizational information on public websites; and the use of organization-provided identifiers and authentication secrets external sites/applications. GSA Order OSC 2106.2, “GSA Social Media Policy,” provides detailed

instructions regarding what GSA personnel can and cannot do regarding the use of social media/networking.

**Contractor System Considerations:** Vendors/contractors must adhere to the control requirements and GSA rules of behavior regarding accessing GSA systems and using social media and external sites/applications.

### 9.2.4 PL-08 Information Security Architecture

**Control:**

a. Develop security and privacy architectures for the system that:
   1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
   2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
   3. Describe how the architectures are integrated into and support the enterprise architecture; and
   4. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures [as necessary, and at least annually in conjunction with SSP reviews/updates] to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| PL-08 | ✓ | ✓ | ✓ | ✓ | ✓ | H | H |

**GSA Implementation Guidance:**
CIO-IT Security-19-95: Security Engineering Architecture Reviews describes GSA's processes for ensuring systems are built in accordance with the Security Engineering Framework to ensure security architectures meet GSA's security requirements and protect GSA systems and data. It includes checklist items that ensure a system's security architecture aligns with GSA's Enterprise Architecture and its approved IT standards and identifies how non-IT standards can be proposed for inclusion in the standards. CIO-IT Security 19-95 includes checklist items regarding the use of external services, systems, and interconnections to GSA.

**Note:** CIO-IT Security-19-95 describes the process to support utilization of new and emergent technologies or when systems undergo major architectural changes to ensure such systems are designed and built or continue to be secure. The system ISSO has the responsibility to notify the ISB Division when changes occur and, as part of the system's annual SSP annual update, consider if any changes have occurred that require architectural review.

System Owners are responsible for ensuring all security architecture changes are reflected in their System Security Plan (SSP), Concept of Operations (CONOPS), criticality analysis, and organizational procedures and procurements/acquisitions (as applicable and/or annually, as part of the system's annual SSP review/update processing).

**Contractor System Considerations:** System Owners, ISSOs, and ISSMs are responsible for ensuring their system architectures are submitted for gaining initial Security and Privacy architectural approval and when significant changes to a system's architecture are planned.

System Owners are responsible for ensuring all security architecture changes are reflected in their SSP, Concept of Operations (CONOPS), criticality analysis, and organizational procedures and procurements/acquisitions, as applicable, and/or annually as part of the system's annual SSP review/update processing.

### 9.2.5 PL-09 Central Management

**Control:**
Centrally manage [common and hybrid security and privacy controls as identified in CIO-IT Security-18-90, Common Control Catalog (CCC)].

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| PL-09 | ✓ | ✓ | ✓ | | | C | C |

**GSA Implementation Guidance:**
Enterprise common and hybrid controls are described in the CCC. GSA system owners, data owners, ISSOs, and ISSMs are responsible for coordinating the inheritance of controls identified in the CCC for their FISMA systems. For hybrid controls, they must implement the system specific portions of the controls as described in the CCC.

**Contractor System Considerations:** Expectations for vendor/contractor systems are specified in the CCC. Most of the controls in the CCC are system-specific or hybrid for vendor/contractor systems, therefore central management of those controls is the responsibility of the vendor/contractor.

### 9.2.6 PL-10 Baseline Selection

**Control:**
Select a control baseline for the system.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| PL-10 | ✓ | ✓ | ✓ | | | H | H |

**GSA Implementation Guidance:**
A system's control baseline is established as described in Section 5.1.4 and summarized below.

A system's FIPS 199 security categorization and the GSA A&A process it follows are used to identify its initial controls from the GSA CTW. If a system contains PII, CUI, PCI data. is designated as an HVA, or includes IT infrastructure the associated overlays for those conditions will be included in the system's baseline.

The System Owner collaborates with the AO, ISSM, ISSO, and Privacy Team as necessary to complete the control selection task, including identifying additional requirements/controls due to a system's business mission or environment as necessary.

**Contractor System Considerations:** Vendor/contractor systems must follow the same process as described above to complete the control baseline selection.

### 9.2.7 PL-11 Baseline Tailoring

**Control:**
Tailor the selected control baseline by applying specified tailoring actions.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| PL-11 | ✓ | ✓ | ✓ | | | H | H |

**GSA Implementation Guidance:**
See Section 5.3.2 for guidance on control tailoring.

**Contractor System Considerations:** System Owners are to collaborate with the ISSM, ISSO, Privacy Team as necessary, and other System Owners (regarding common/hybrid controls) to complete their assigned system's control tailoring requirements.

## 9.3 Risk Assessment (RA)

### 9.3.1 RA-01 Policy and Procedures

**Control:**

a. Develop, document, and disseminate to [personnel with IT security responsibilities as defined in GSA CIO Order 2100.1]:
   1. [Organization-level] risk assessment policy that:
   (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the planning policy and the associated risk assessment controls;
b. Designate an [CISO] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and
c. Review and update the current risk assessment:
   1. Policy [review annually and update as necessary] and following [changes to Federal or GSA policies, requirements, or guidance]; and
   2. Procedures [at least every three (3) years] and following [changes to Federal or GSA policies, requirements, or guidance].

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| RA-01 | ✓ | ✓ | ✓ | | | C | H |

**GSA Implementation Guidance:**
The GSA risk assessment policy is defined in the GSA Order CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for risk assessment activities. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency Directives website.

Risk assessment procedures are documented in CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk and other procedural guides referenced in it. The procedures facilitate the

implementation of the risk assessment policy and associated controls. All GSA procedural guides are disseminated GSA-wide via GSA's InSite centralized agency IT Security Procedural Guides Library website.

The GSA OCISO is responsible for managing the development, documentation, and dissemination of all GSA IT security policies procedural guides.

The GSA OCISO is responsible for reviewing 2100.1 annually and updating it as necessary, and following changes to Federal or GSA policies, requirements, or guidance.

The GSA OCISO is responsible for reviewing and updating CIO-IT Security-06-30 and all procedural guides at least every three (3) years and following changes to Federal or GSA policies, requirements, or guidance.

**Contractor System Considerations:** Vendors/Contractors must use GSA policies and guides regarding risk assessment policies and procedures. They may supplement them with their own risk assessment policies and procedures with the approval of the GSA CISO and AO.

### 9.3.2 RA-02 Security Categorization

**Control:**

a. Categorize the system and information it processes, stores, and transmits;
b. Document the security categorization results, including supporting rationale, in the security plan for the system; and
c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| RA-02 | ✓ | ✓ | ✓ | | ✓ | S | S |

**GSA Implementation Guidance:**
GSA system owners, data owners, ISSOs, and ISSMs are required to follow the processes and procedures described in:

- Section 5.2.2: System Categorization of this guide for determining the security categorization of their information and information systems; and
- Section 5.2.3: System Categorization Review and Approval of this guide for approval of the security categorization of their information and information systems.

**Contractor System Considerations:** Vendor/contractor systems must follow the same processes and procedures for determining the security categorization of their information and information systems and its approval as described above.

### 9.3.3 RA-03 Risk Assessment

**Control:**

a. Conduct a risk assessment, including:
    1. Identifying threats to and vulnerabilities in the system;

2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;
c. Document risk assessment results in [a security assessment report (SAR) or as specified in CIO-IT Security-06-30 and GSA's other Assessment and Authorization processes identified therein];
d. Review risk assessment results [as specified in CIO-IT Security-06-30 and GSA's other Assessment and Authorization processes identified therein];
e. Disseminate risk assessment results to [personnel with risk assessment/management responsibilities as defined in GSA CIO Order 2100.1]; and
f. Update the risk assessment [as specified in CIO-IT Security-06-30 and GSA's other Assessment and Authorization processes identified therein] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

**Control Enhancements:**

(01) Risk Assessment | Supply Chain Risk Assessment –
(a) Assess supply chain risks associated with [GSA SSO or Contractor recommended systems, system components, and system services as approved by the CISO and AO]; and
(b) Update the supply chain risk assessment [GSA SSO or Contractor recommended frequency as approved by the CISO and AO], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| RA-03 | ✓ | ✓ | ✓ | | ✓ | H | H |
| RA-03(01) | ✓ | ✓ | ✓ | | | C | S |

**GSA Implementation Guidance:**

CIO 2100.1 and this guide require risk assessments to be performed as part of the initial A&A of GSA information systems, including identifying threats and likelihoods of harm and impact to systems.

CIO-IT Security-18-91 describes how GSA integrates risk management across the organizational, mission/business, and information system levels.

This guide requires a Security Assessment Report (SAR), or similar assessment of risk be prepared based on which A&A process a system uses.

This guide requires risk assessments to be reviewed in accordance with the GSA authorization process used. Risk assessment results (e.g., the SAR) are provided to security personnel responsible for the security of a GSA system as part of the A&A package during initial authorization and subsequent updates to the system's authorization and operation. Assessments must be updated based on which A&A process a system uses and if a significant

change to the system, its environment, or its risk posture is identified during monitoring or annual updates of the system's A&A package.

The system ISSO, ISSM, and System Owner are responsible for ensuring their system risk assessments are reviewed, updated, and disseminated in accordance with GSA policies and guides.

As per RA-03(01), the OCISO Cyber Supply Chain Risk Management (C-SCRM) team develops, maintains, and annually updates a list of critical suppliers for GSA-IT. The list is based on input from various sources for GSA-IT managed systems. It includes software inventories, hardware inventories, and financials related to acquisitions. Supply chain risks that are unique for the most critical vendors, are then incorporated into final determinations. For the resultant set of critical vendors supplier assessments are conducted and significant risks are addressed. The specific controls for maintaining the critical supplier list and conducting supplier reviews are identified within the C-SCRM Program's Standard Operating Procedures (SOPs).

**Contractor System Considerations:** Vendor/contractor systems must follow the same processes and procedures for conducting risk assessments as described above. System Owners must establish a process and perform system-specific or organization-wide Supplier Assessments and Reviews consistent with NIST SP 800-161r1-upd1, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations."

### 9.3.4 RA-05 Vulnerability Monitoring and Scanning

**Control:**

a. Monitor and scan for vulnerabilities in the system and hosted applications [weekly authenticated scans for operating systems (OS)-including databases, monthly unauthenticated scans for web application, annual authenticated scans for web applications] and when new vulnerabilities potentially affecting the system are identified and reported;
b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from vulnerability monitoring;
d. Remediate legitimate vulnerabilities [within:

    - 14 days for CISA Known Exploitable Vulnerabilities (KEV)
    - 15 days for Critical vulnerabilities for Internet-accessible systems or services
    - 30 days for Critical and High vulnerabilities
    - 90 days for Moderate vulnerabilities
    - 180 days for Low vulnerabilities.]

    in accordance with an organizational assessment of risk;
e. Share information obtained from the vulnerability monitoring process and control assessments with [ISSOs] to help eliminate similar vulnerabilities in other systems; and
f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

**Control Enhancements:**

(02) Vulnerability Monitoring and Scanning | Update Vulnerabilities to be Scanned – Update the system vulnerabilities to be scanned [continuously – before each scan].
(04) Vulnerability Monitoring and Scanning | Discoverable Information – Determine information about the system that is discoverable and take [GSA SSO recommended and GSA CISO and AO approved corrective actions]
(05) Vulnerability Monitoring and Scanning | Privileged Access - Implement privileged access authorization to [all information system components as applicable (e.g., OS, DB, Web App, etc.] for [all vulnerability scanning activities].
(11) Vulnerability Monitoring and Scanning | Public Disclosure Program – Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| RA-05 | ✓ | ✓ | ✓ | ✓ | ✓ | H | S |
| RA-05(02) | ✓ | ✓ | ✓ | | | C | S |
| RA-05(04) | | | ✓ | | | S | S |
| RA-05(05) | | ✓ | ✓ | | ✓ | H | S |
| RA-05(11) | ✓ | ✓ | ✓ | | | S | S |

**GSA Implementation Guidance:**
CIO-IT Security-17-80: Vulnerability Management Process describes the requirements for vulnerability scanning of GSA information systems and applications. It also describes an ad hoc process which can be used to scan for new vulnerabilities. CIO-IT Security-17-80 describes the scanning tools and techniques GSA uses to automate, as much as is possible, the scanning of GSA information systems and applications. It includes a description of the use of the Common Vulnerability Scoring System (CVSS) for assigning risks for tools that support CVSS. CIO-IT Security-17-80 assigns ISSOs the responsibility to evaluate and analyze scan reports and results in collaboration with information system personnel. GSA Order CIO 2100.1, this guide, and CIO-IT Security-17-80 all require remediation based on the time periods in the RA-05, Part b parameter. Tools used at GSA can be readily updated to identify new or newly exploited vulnerabilities, dependent upon the ability of the tool to identify vulnerabilities on assets.

CIO-IT Security-17-80 describes how the different reports or dashboards are shared with ISSOs, ISSMs, and executives as necessary. Reports such as the Top 10 vulnerability summaries can be used to identify systemic issues across GSA.

As per RA-05(02), the scanning tools used by GSA's ISB Division are scheduled for auto-updates daily and update the tool configuration as necessary before running scans.

As per RA-05(04), GSA's ISB Division shares reports and dashboards with ISSOs who must coordinate with system personnel to take corrective actions to restrict discoverable information about systems as necessary.

As per RA-05(05), GSA FIPS 199 High Impact systems must collaborate with the ISB Division to implement privileged access to system assets in support of the vulnerability scanning capabilities described in CIO-IT Security-17-80.

As per RA-05(11), GSA's Vulnerability Disclosure Policy establishes GSA's public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

**Contractor System Considerations:** Vendors/contractors must adhere to GSA policies and guides and comply with the control requirements vulnerability monitoring and scanning.

### 9.3.5 RA-07 Risk Response

**Control:** Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| RA-07 | ✓ | ✓ | ✓ | | | S | S |

**GSA Implementation Guidance:**
ISSOs, System Owners, and system, network, and database administrators, will coordinate and perform remediation actions based upon the results of ongoing monitoring activities, assessment of risk, and outstanding items in the system's POA&M as described in Section 5.7.3 of this guide.

**Contractor System Considerations:** Vendors/contractors must adhere to GSA policies and guides and comply with the control requirements regarding risk response.

### 9.3.6 RA-08 Privacy Impact Assessments

**Control:** Conduct privacy impact assessments for systems, programs, or other activities before:

a. Developing or procuring information technology that processes personally identifiable information; and
b. Initiating a new collection of personally identifiable information that:
   1. Will be processed using information technology; and
   2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

**Note:** RA-08 is included in all FIPS 199 Baselines to ensure all systems complete a Privacy Threshold Assessment (PTA) to determine if a Privacy Impact Assessment (PIA) is required.

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| RA-08 | ✓ | ✓ | ✓ | ✓ | ✓ | H | H |

**GSA Implementation Guidance:**
The GSA's Privacy Program website provides guidance on conducting Privacy Impact Assessments (PIAs), including a link to GSA Order CIO 1878.3, "Developing and Maintaining Privacy Threshold Assessments (PTAs), PIAs, Privacy Act Notices, and System of Records Notices." 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 review and

update them in alignment with the systems ATO authorization cycle and/or when there is a significant change to the system. GSA's GRC tool is used to complete PTAs and PIAs for GSA's FISMA systems.

**Contractor System Considerations:** Vendors/contractors must adhere to GSA policies and guides and comply with the control requirements regarding PTAs and PIAs.

### 9.3.7 RA-09 Criticality Analysis

**Control:** Identify critical system components and functions by performing a criticality analysis for [all systems as part of their Business Impact Analysis (BIA)] at [initial system design and development and throughout its lifecycle to ensure any criticality changes are identified].

| | Low | Mod | High | LATO | MiSaaS | Federal | Contractor |
|---|---|---|---|---|---|---|---|
| RA-09 | | ✓ | ✓ | | | S | S |

**GSA Implementation Guidance:**
GSA system owners, data owners, ISSOs, and ISSMs must identify the criticality of components as part of the Business Impact Analysis (BIA) included in Contingency Planning (CP) activities. Throughout a system's lifecycle as changes to the system occur, they must be analyzed to determine if the criticality of the system or its components has changed. If changes have occurred, the BIA and CP Plan for the system must be updated.

**Contractor System Considerations:** Vendors/contractors must adhere to GSA policies and guides and comply with the control requirements regarding criticality analysis.

# Appendix A: Consolidated List of Guidance, Policies, Procedures, Templates

**Federal Laws/Regulations/Guidance:**

- CISA Cybersecurity Directives
- EO 13800, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- FIPS 140-2, Security Requirements for Cryptographic Modules
- FIPS 140-3, Security Requirements for Cryptographic Modules
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST Cybersecurity Framework (CSF) 2.0
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal 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 800-47, Revision 1, Managing the Security of Information Exchanges
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-53B, Control Baselines 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 800-161r1-upd1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- NIST SP 800-171r3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST SP 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements
- Public Law 113-283, Federal Information Security Modernization Act of 2014
- Public Law 116-207, Internet of Things Cybersecurity Improvement Act of 2020

**GSA Policies and Guidance:**

- GSA MV-2023-02, Supplements 1-2, Ensuring Only Approved Software is Acquired and Used at GSA

The GSA policies listed below are available on the GSA.gov Directives Library page.

- GSA Order CIO 1878.3, Developing and Maintaining Privacy Threshold Assessments (PTAs), PIAs, Privacy Act Notices, and System of Records Notices
- GSA Order CIO 2100.1, GSA Information Technology (IT) Security Policy
- GSA Order CIO 2101.3, GSA Integrated Information Technology Management
- GSA Order CIO 2104.1, GSA Information Technology (IT) General Rules of Behavior
- GSA Order OSC 2106.2, GSA Social Media Policy
- GSA Order 2160.1, GSA Information Technology (IT) Standards Policy

- GSA Order CIO 2183.1, Enterprise Identity, Credential, and Access Management (ICAM) Policy

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page.

- GSA CIO-IT Security-01-05: Configuration Management (CM)
- GSA CIO-IT Security-04-26: Federal Information Security Modernization Act (FISMA) Implementation Process
- GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk
- GSA CIO-IT Security-06-32: Media Protection (MP)
- GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts
- GSA CIO-IT Security-11-51: Conducting Penetration Test Exercises
- GSA CIO-IT Security-11-62: Salesforce Platform Security Implementation
- GSA CIO-IT Security-14-68: Lightweight Security Authorization Process
- GSA CIO-IT Security-16-75: Low Impact Software as a Service (LiSaaS) Solutions Authorization Process
- GSA CIO-IT Security-18-88: Moderate Impact Software as a Service (MiSaaS) Security Authorization Process
- GSA CIO-IT Security-18-91: Risk Management Strategy (RMS)
- GSA CIO-IT Security-19-95: Security Engineering Architecture Reviews
- GSA CIO-IT Security-20-106: GSA Pages Site Review and Approval Process
- GSA CIO-IT Security-21-117: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program
- GSA CIO-IT Security-24-125: Managing Information Exchange Agreements
- GSA CIO-IT Security-26-148: Managing High Value Assets

The GSA CIO-IT Security Procedural Guides listed below are only available on the internal GSA InSite IT Security Procedural Guides page.

- CIO-IT Security-01-08: Auditing and Accountability (AU)
- GSA CIO-IT Security-07-35: Web Application Security
- GSA CIO-IT Security-08-39: FYxx IT Security Program Management Implementation Plan
- GSA CIO-IT Security-09-44: Plan of Action and Milestones (POA&M)
- GSA CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program
- GSA CIO-IT Security-14-69: SSL/TLS Implementation
- CIO-IT Security-16-76: Building Monitoring and Control (BMC) Systems Security Assessment Process
- GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC)
- GSA CIO-IT Security-19-97: Robotic Process Automation (RPA) Security
- GSA CIO-IT Security-19-101: External Information System Monitoring
- GSA CIO-IT Security-12-67: Securing Mobile Applications and Devices
- GSA CIO-IT Security-21-112: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations Process
- GSA CIO-IT Security-21-120: Supply Chain Risk Management (SR) Controls
- GSA CIO-IT Security-24-130: Conducting Red Team Exercises

The GSA CIO-IT Security Forms (document templates) listed below are available on the InSite IT Security Forms and Aids web page.

- FIPS 199 Security Categorization Template
- Digital Identity Acceptance Statement
- GSA Control Tailoring Workbook
- Control Implementation Summaries
- System Security Plan (SSP) Templates
- Security Assessment Plan (SAP) Templates
- GSA Test Case Workbooks
- Security Assessment Report (SAR) Templates
- Certification Letter Templates
- ATO/Approval Letter Templates
- Contingency Plan Templates
- Contingency Plan Test Plan Template
- Contingency Plan Test Report Template
- Information Exchange Agreement/ Memorandum of Agreement (IEA/MOA) Templates
- Information Security Agreement/Memorandum of Agreement (ISA/MOA) Templates
- Penetration Test Exercise Templates
- POA&M Share Drive User Access Request Form
- ISCM Ongoing Authorization Templates
- Salesforce Application Templates
- Transfer Notification Template
- Disposal Notification Template
- Policy Deviation Memorandum for Record
- Attestation Letter templates
- Checklist templates
- CUI Nonfederal System Templates
- Incident Response Templates
- RPA Templates
- Vendor (External Information System) Templates
- Configuration Management Templates
- Red Team Templates
- Media Protection Templates

Privacy Threshold Assessment/Privacy Impact Assessment information is available on GSA's IT Privacy page.

## Appendix B: Critical Controls

Table B-1 outlines Critical NIST SP 800-53 controls identified by GSA. Systems not fully compliant with these controls will not receive full Authority to Operate (ATO); instead, a time-bound Conditional ATO will be issued.

### Table B-1. Critical Controls

| # | Description | Control Reference |
|---|---|---|
| 1 | **Multi-Factor Authentication (MFA) for Privileged & User-level access**:<br>All systems shall utilize a GSA-approved multi-factor authentication mechanism for both privileged and non-privileged user authentication. All new and modernizing systems must undergo an ICAM Portfolio Review in accordance with GSA Order CIO 2183.1, "Enterprise Identity, Credential, and Access Management (ICAM) Policy."<br>If an assessment identifies MFA has not been implemented, per policy requirements, then the system will not be approved for a 3-year ATO or OA, until MFA is implemented. | IA-02(01) Identification and Authentication (Organizational Users) \| Multifactor Authentication to Privileged Accounts<br>IA-02(02) Identification and Authentication (Organizational Users) \| Multifactor Authentication to Non-Privileged Accounts |
| 2 | **Critical and High Vulnerabilities**:<br>GSA requires ongoing remediation actions including patching, updating, and upgrading out of date components, addressing known vulnerabilities, completing POA&Ms, and maintaining secure configurations of components.<br>If an assessment identifies ongoing remediation actions that are not being addressed within the remediation timeline as defined in CIO-IT Security-17-80: Vulnerability Management, then the system will not be approved for a 3-year ATO or OA, until the associated risks are mitigated. | SI-02 Flaw Remediation |
| 3 | **Remote Code Execution (RCE) Vulnerabilities**:<br>RCE vulnerabilities can be exploited if user input is injected into a File or a String and executed (evaluated) by the programming language's parser. RCE vulnerabilities must be remediated, regardless of the RCE system impact level identified.<br>If an information system is identified with an RCE vulnerability during an assessment, then the system will not be approved for a 3-year ATO or OA, until the risk is mitigated. | SI-02 Flaw Remediation |
| 4 | **EOL Software**:<br>The continued usage of End of Life (EOL) Software requires a risk evaluation to be performed by the OCISO. An EOL Software usage justification to include POA&M tracking requirements or an approved | SA-22 Unsupported System Components |

| # | Description | Control Reference |
|---|---|---|
| | Acceptance of Risk (AOR), are the possible documentation outcome requirements of the risk evaluation.<br><br>If an assessment identifies EOL software usage has not been properly evaluated and documented, then the system will not be approved for a 3-year ATO or OA, until completed. | |
| **5** | **System Architecture has been reviewed and approved by ISB:**<br><br>CIO-IT Security-19-95: Security Engineering Architecture Reviews identifies the OCISO ISB Division system evaluation requirements.<br><br>If an assessment identifies an ISB security engineering architecture review has not been completed for the system, then the system will not be approved for a 3-year ATO or OA, until one is completed. | PL-08 Security and Privacy Architecture<br><br>SA-17 Developer Security and Privacy Architecture and Design |
| **6** | **Integration with GSA's Security Stack (Federal Systems)**:<br><br>System integration includes;<br><br>● Sending all logs listed in CIO-IT Security-01-08: Auditing and Accountability (AU) to GSA's central Enterprise Logging Platform (ELP) to support information system monitoring.<br>● Retaining logs for a minimum of 12 months online and 18 months in cold storage.<br>● Using GSA OCISO perimeter firewall services.<br>● Integration with GSA's internal infrastructure security tools (agent and agent-less) for:<br>○ Configuration setting monitoring (e.g., BigFix, MaaS360, GoogleMDM, Prisma Cloud Enterprise).<br>○ Whitelisting/blacklisting and restricting user installation of software (e.g., CarbonBlack).<br>○ Scanning to identify vulnerabilities (e.g., Tenable Security Center (TSC), Invicti).<br>○ Antivirus and malicious code protection (e.g., FireEye HX, Endgame/Elastic Security Defend).<br>○ Inventory management (e.g., BigFix, MaaS360, GoogleMDM, Prisma Cloud Enterprise). Integration with GSA's security container-based management solutions<br>● Cloud Service Provider Integrations (e.g., Prisma Cloud Enterprise).<br><br>**Note:** The tools referenced above relate to GSA's internal infrastructure and systems those tools can be integrated with, including tools used within GSA's cloud environments. Additional tools providing the same function may be used in Contractor systems if approved by the GSA CISO and AO.<br><br>If an assessment identifies a system that has not been integrated with GSA Security Stack (based upon the specific system requirements), then the system will not be approved for a 3-year ATO or OA, until the deployment requirements have been completed. | Additional details on GSA's security stack can be found in this Google Sheet.<br><br>GSA ISCM Enterprise Security Management Tools |

| # | Description | Control Reference |
|---|---|---|
| 7 | **Encryption of Sensitive Data (i.e., PII, PCI, Authenticators, other business sensitive data):**<br><br>**Encryption of Sensitive Data at Rest**<br><br>**Systems that process Personally Identifiable Information (PII), Payment Card Industry (PCI) data, Authenticators (e.g., passwords, tokens, keys, certificates, hashes, etc.), and other sensitive data as determined by the AO, shall encrypt that data everywhere (i.e., at file level, database level, at rest, and in transit). All databases must be encrypted. Encryption of the whole database and at the table, column, or field levels containing the sensitive data is required. Methods including, but not limited to, application encryption or tokenization are also acceptable.<br><br>**Encryption of Sensitive Data in Transit**<br><br>For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer, Firewall, and/or WAF shall employ re-encryption techniques to ensure end to end encryption.**<br><br>ALL associated URLs must have their second-level domain HTTP Strict Transport Security (HSTS) preloaded and have no weak ciphers, have no weak protocols, and preload .gov domains. (see BOD 18-01, Enhance Email and Web Security).<br><br>SSL/TLS implementations shall align with CIO-IT Security-14-69: SSL/TLS Implementation.<br><br>**GSA Policy for FIPS 140-3/140-2 Encryption Modules and FIPS-approved encryption ciphers**<br><br>GSA requires the use of FIPS 140-3[4] validated encryption modules and FIPS-approved ciphers for GSA sensitive data at rest and in transit (e.g., PII, PCI, Authenticators, other business sensitive data). Any exceptions must be documented in an Acceptance of Risk (AOR) signed by the GSA CISO and AO.<br><br>If an assessment identifies the system has not addressed data encryption based upon the specific system's data protection requirements, then the system will not be approved for a 3-year ATO or OA, until the deployment requirements have been completed. | SC-08 Transmission Confidentiality and Integrity<br><br>SC-08(01) Transmission Confidentiality and Integrity \| Cryptographic Protection<br><br>SC-28 Protection of Information at Rest<br><br>SC-28(01) Protection of Information at Rest \| Cryptographic Protection |
| 8 | **Compliance with CISA EDs/BODs:**<br><br>CISA develops and oversees the implementation of BODs and EDs which require action to safeguard Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; and protecting the information system from, or mitigating, an information security threat. | SI-02 Flaw Remediation |

[4] NIST has issued FIPS 140-3 and no longer accepts FIPS 140-2 modules for validation. However, previously validated 140-2 modules will be accepted through September 22, 2026. For additional information see the NIST cryptographic module validation program web page.

| # | Description | Control Reference |
|---|---|---|
| | BODs and EDs are compulsory. Federal agencies are required to comply per 44 U.S.C. § 3552 (b)(1)(A)(B)(C) and 44 U.S.C. § 3554 (a)(1)(B)(v).<br><br>If an assessment identifies a system has not complied with CISA BODs/EDs, including the CISA KEV Catalog vulnerabilities per BOD 26-04, and does not have approved AORs for any shortfalls, then the system will not be approved for an ATO. | |

## Appendix C: CSF Function, Category, and Subcategory Definitions

This appendix is based on NIST CSF 2.0.

The six CSF core functions are:

- **Govern (GV):** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- **Identify (ID):** The organization's current cybersecurity risks are understood.
- **Protect: (PR):** Safeguards to manage the organization's cybersecurity risks are used.
- **Detect (DE):** Possible cybersecurity attacks and compromises are found and analyzed.
- **Respond (RS):** Actions regarding a detected cybersecurity incident are taken.
- **Recover (RC):** Assets and operations affected by a cybersecurity incident are restored.

Table C-1 lists how the NIST CSF 2.0 has mapped its functions to NIST SP 800-37, Revision 2 steps and tasks.

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

| CSF Function | Mapped RMF Steps and Tasks |
|---|---|
| **Govern (GV)** | **Prepare Step:**<br>Task P-1: Risk Management Roles<br>Task P-2: Risk Management Strategy<br>Task P-3: Risk Assessment – Organization<br>Task P-7: Continuous Monitoring Strategy<br>Task P-8: Mission or Business Focus<br>Task P-9: System Stakeholders<br>Task P-10: Asset Identification<br>Task P-14: Risk Assessment – System<br>Task P-15 Requirements Definition<br>**Select Step:**<br>Task S-5: Continuous Monitoring Strategy – System<br>**Assess Step:**<br>Task A-3: Control Assessments<br>Task A-5: Remediation Actions<br>Task A-6: Plan of Action and Milestones<br>**Authorize Step:**<br>Task R-2: Risk Analysis and Determination<br>Task R-3 Risk Response<br>**Monitor Step:**<br>Task M-1: System and Environment Changes<br>Task M-2: Ongoing Assessments<br>Task M-3: Ongoing Risk Response<br>Task M-7 System Disposal |
| **Identify (ID)** | **Prepare Step:**<br>Task P-2: Risk Management Strategy<br>Task P-3: Risk Assessment – Organization<br>Task P-6: Impact-Level Prioritization (Optional)<br>Task P-7: Continuous Monitoring Strategy – Organization<br>Task P-8: Mission or Business Focus<br>Task P-10: Asset Identification<br>Task P-11: Authorization Boundary<br>Task P-12: Information Types<br>Task P-13: Information Life Cycle |

| CSF Function | Mapped RMF Steps and Tasks |
|---|---|
| | Task P-14: Risk Assessment – System<br>Task P-15 Requirements Definition<br>Task P-16: Enterprise Architecture<br>**Categorize Step:**<br>Task C-2: Security Categorization<br>Task C-3: Security Categorization Review and Approval<br>**Select Step:**<br>Task S-4: Documentation of Planned Control Implementations<br>**Implement Step:**<br>Task I-2: Update Control Implementation Information<br>**Assess Step:**<br>Task A-3: Control Assessments<br>Task A-4: Assessment Reports<br>Task A-5: Remediation Actions<br>Task A-6: Plan of Action and Milestones<br>**Authorize Step:**<br>Task R-2: Risk Analysis and Determination<br>Task R-3: Risk Response<br>Task R-4: Authorization Decision<br>Task R-5: Authorization Reporting<br>**Monitor Step:**<br>Task M-1: System and Environment Changes<br>Task M-2: Ongoing Assessments<br>Task M-3: Ongoing Risk Response<br>Task M-5: Security and Privacy Reporting<br>Task M-6: Ongoing Authorization<br>Task M-7: System Disposal |
| **Protect (PR)** | **Prepare Step:**<br>Task P-2: Risk Management Strategy<br>Task P-15: Requirements Definition<br>Task P-16: Enterprise Architecture<br>Task P-17: Requirements Allocation |
| **Detect (DE)** | **Monitor Step:** The CSF does not identify specific tasks. |
| **Respond (RS)** | **Monitor Step:**<br>Task M-3: Ongoing Risk Response |
| **Recover (RC)** | **Prepare Step:**<br>Task P-2: Risk Management Strategy<br>**Monitor Step:**<br>Task M-3: Ongoing Risk Response |
| **Not Mapped to any CSF Function** | **Prepare Step:**<br>Task P-4: Organizationally – Tailored Control Baselines and Cybersecurity Framework Profiles (Optional)<br>Task P-5: Common Control Identification<br>Task P-18: System Registration<br>**Categorize Step:**<br>Task C-1: System Description<br>**Select Step:**<br>Task S-1: Control Selection<br>Task S-2: Control Tailoring<br>Task S-3: Control Allocation<br>Task S-6: Plan Review and Approval<br>**Implement Step:**<br>Task I-1: Control Implementation |

| CSF Function | Mapped RMF Steps and Tasks |
|---|---|
| | **Assess Step:**<br>Task A-1: Assessor Selection<br>Task A-2: Assessment Plan<br>**Authorize Step:**<br>Task R-1: Authorization Package<br>**Monitor Step:**<br>Task M-4: Authorization Package Updates<br>Task M-5: Security and Privacy Reporting |

Table C-2 lists the Functions and Categories (e.g., GV, GV.OC) and Subcategories (GV.OC-03) from the CSF that are identified as related to the implementation of policies, procedures, and processes regarding the NIST SP 800-53 control families documented in this guide: Assessment, Authorization, and Monitoring (CA), Planning (PL), and Risk Assessment (RA). The NIST 800-53 controls are listed in parentheses in the Definition/Description column (e.g., CA-07). The CSF Recover (RC) function is not mapped to any CA, PL, or RA controls, therefore it is not listed in the table.

### Table C-2. CSF Categories/Subcategories and the CA, PL, and RA Controls

| CSF Function/Category | Definition/Description |
|---|---|
| **Govern (GV)** | The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. |
| **Organizational Context (GV.OC):** The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood | **GV.OC-03:** Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed (CA-01, PL-01, RA-01) |
| **Policy (GV.PO):** Organizational cybersecurity policy is established, communicated, and enforced | **GV.PO-01:** Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced (CA-01, PL-01, RA-01)<br>**GV.PO-02:** Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission (CA-01, PL-01, RA-01) |
| **Oversight (GV.OV):** Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy | **GV.OV-01:** Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction (CA-01, PL-01, RA-01, RA-07) |
| **Cybersecurity Supply Chain Risk Management (GV.SC):** Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders | **GV.SC-03:** Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (CA-01, PL-01, RA-01, RA-03, RA-07) |

| CSF Function/Category | Definition/Description |
|---|---|
| **Identify (ID)** | The organization's current cybersecurity risks are understood. |
| **Improvement (ID.AM):** Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy | **ID.AM-03:** Representations of the organization's authorized network communication and internal and external network data flows are maintained (CA-03, CA-09, PL-02, PL-08)<br>**ID.AM-05:** Assets are prioritized based on classification, criticality, resources, and impact on the mission (RA-02, RA-03, RA-09)<br>**ID.AM-08:** Systems, hardware, software, services, and data are managed throughout their life cycles (PL-02) |
| **Risk Assessment (ID.RA):** The cybersecurity risk to the organization, assets, and individuals is understood by the organization | **ID.RA-01:** Vulnerabilities in assets are identified, validated, and recorded (CA-02, CA-07, CA-08, RA-03, RA-05)<br>**ID.RA-03:** Internal and external threats to the organization are identified and recorded (RA-03)<br>**ID.RA-04:** Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded (RA-02, RA-03, RA-08, RA-09)<br>**ID.RA-05:** Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization (RA-02, RA-03, RA-07)<br>**ID.RA-06:** Risk responses are chosen, prioritized, planned, tracked, and communicated (RA-07)<br>**ID.RA-07:** Changes and exceptions are managed, assessed for risk impact, recorded, and tracked (CA-07)<br>**ID.RA-08:** Processes for receiving, analyzing, and responding to vulnerability disclosures are established (RA-05) |
| **Improvement (ID.IM):** Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions | **ID.IM-01:** Improvements are identified from evaluations*<br>**ID.IM-02:** Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties*<br>**ID.IM-03:** Improvements are identified from execution of operational processes, procedures, and activities*<br>**ID.IM-04:** Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved*<br>***The CA, PL, and RA controls listed below are mapped to a CSF function, therefore all are in scope for improvements per this category. (CA-01,CA-02, CA-03, CA-05, CA-07, CA-08, CA-09, PL-01, PL-02, PL-08, RA-01, RA-02, RA-03, RA-05, RA-07, RA-08, RA-09) |

| CSF Function/Category | Definition/Description |
|---|---|
| **Protect (PR)** | Safeguards to manage the organization's cybersecurity risks are used. |
| **Data Security (PR.DS):** Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information | **PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected (CA-03)<br>**PR.DS-02:** The confidentiality, integrity, and availability of data-in-transit are protected (CA-03)<br>**PR.DS-10:** The confidentiality, integrity, and availability of data-in-use are protected (CA-03) |
| **Detect (DE)** | Possible cybersecurity attacks and compromises are found and analyzed. |
| **Continuous Monitoring (DE.CM)**: Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events | **DE.CM-01:** Networks and network services are monitored to find potentially adverse events (CA-07)<br>**DE.CM-02:** The physical environment is monitored to find potentially adverse events (CA-07)<br>**DE.CM-03:** Personnel activity and technology usage are monitored to find potentially adverse events (CA-07)<br>**DE.CM-06:** External service provider activities and services are monitored to find potentially adverse events (CA-07)<br>**DE.CM-09:** Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events (CA-07) |
| **Adverse Event Analysis (DE.AE)**: Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents | **DE.AE-02:** Potentially adverse events are analyzed to better understand associated activities (CA-07)<br>**DE.AE-03:** Information is correlated from multiple sources (CA-07)<br>**DE.AE-06**: Information on adverse events is provided to authorized staff and tools (RA-03)<br>**DE.AE-07**: Cyber threat intelligence and other contextual information are integrated into the analysis (RA-03) |
| **Respond (RS)** | Actions regarding a detected cybersecurity incident are taken. |
| **Incident Analysis (RS.AN)**: Investigations are conducted to ensure effective response and support forensics and recovery activities | **RS.AN-08:** An incident's magnitude is estimated and validated (RA-03, RA-07) |

## Appendix D: A&A Process Package Document Lists/Links

This Appendix contains a listing of the A&A Package documentation requirements for each of the A&A processes described in this guide. Document templates are available on the InSite IT Security Forms and Aids web page. Search for the title of the document listed to obtain its current version.

**Note:** The GSA is in the process of implementing its A&A processes into its GRC tool. The GRC tool is used as a data and document repository for systems' A&A information. Documents required for a system's ATO may reside or be generated within the GRC tool, or may be produced outside of the tool and uploaded to a system's A&A Repository within the tool. In either case, the documents listed in the following tables must be in the GRC tool. Any questions regarding the use of GSA's GRC tool should be sent to archersupport@gsa.gov.

| **Standard A&A Process** |
|---|
| **Authorization Package Documents** |
| ● System Security Plan (Low, Moderate, High, or HVA)<br>● Security Assessment Report<br>● Certification Letter<br>● ATO Letter<br>● Plan of Action and Milestones |
| **Other Required Documents (as noted)** |
| ● **ATO Related Documents**<br>○ Privacy Threshold Assessment/Privacy Impact Assessment<br>○ FIPS 199 Security Categorization<br>○ Digital Identity Acceptance Statement<br>○ Interconnection Security Agreement(s)/Information Exchange Agreements (if applicable)<br>○ Control Tailoring Workbook (CTW)<br>○ Control Implementation Summary<br>○ Contingency Plan (with Business Impact Assessment)<br>○ Contingency Plan Test Report<br>○ Incident Response Plan<br>○ Incident Response Plan Test Report<br>○ Configuration Management Plan (Moderate and High only)<br>○ Code Review Report (if applicable)<br>● **Assessment Related Documents**<br>○ Security Assessment Plan (SAP)<br>○ GSA NIST SP 800-53, Revision 5 Test Case Workbook<br>○ Authenticated OS Vulnerability Scan Results<br>○ Authenticated Web Application Vulnerability Scan Results<br>○ Penetration Test Report (if applicable)<br>○ Red Team Exercise Report (if applicable) |

| Lightweight Security Authorization Process |
|---|
| **90-Day LATO** |
| **Authorization Package Documents** |
| ● Vulnerability Scan Results<br>● Certification Letter<br>● ATO Letter<br>● Plan of Action and Milestones |
| **Other Required Documents (as noted)** |
| ● Privacy Threshold Assessment/Privacy Impact Assessment<br>● FIPS 199 Security Categorization<br>● Digital Identity Acceptance Statement<br>● Architecture review conducted by ISB<br>● Penetration Test Results (if applicable) |
| **One Year LATO, Three Year LATO** |
| **Authorization Package Documents** |
| ● System Security Plan<br>● Security Assessment Report<br>● Certification Letter<br>● ATO Letter<br>● Plan of Action and Milestones<br>● Customer Responsibility Matrix (CRM) - Please contact the designated ISSM to receive the vendor's current CRM for the system. (if applicable) |
| **Other Required Documents (as noted)** |
| ● Privacy Threshold Assessment/Privacy Impact Assessment<br>● FIPS 199 Security Categorization<br>● Control Implementation Summary<br>● Digital Identity Acceptance Statement<br>● Vulnerability Scan Results<br>● Code Review Report (if applicable)<br>● Penetration Test Results (if applicable) |

| Security Reviews for Low Impact Software as a Service Solutions Process |
|---|
| **Authorization Package Documents** |
| ● LiSaaS Solution Profile<br>● LiSaaS Solution Review Checklist<br>○ Checklist Supporting Artifacts<br>● FIPS 199 Categorization<br>● Privacy Threshold Assessment<br>● Latest vulnerability scan results (e.g., web, OS, container), as applicable<br>● LiSaaS Attestation Letter (if applicable)<br>● ATO Letter |

| Moderate Impact Software as a Service (MiSaaS) Security Authorization Process |
|---|
| **Authorization Package Documents** |
| ● System Security Plan<br>● Security Assessment Report<br>● Certification Letter<br>● ATO Letter<br>● Plan of Action and Milestones<br>● Customer Responsibility Matrix(CRM) - Please contact the designated ISSM to receive the vendor's current CRM for the system. |
| **Other Required Documents (as noted)** |
| ● **ATO Related Documents**<br>○ Privacy Threshold Assessment/Privacy Impact Assessment<br>○ FIPS 199 Security Categorization<br>○ Digital Identity Acceptance Statement<br>○ Interconnection Security Agreement(s)/Information Exchange Agreements (if applicable)<br>○ Control Tailoring Workbook (CTW)<br>○ Control Implementation Summary<br>○ Contingency Plan (with Business Impact Assessment)<br>○ Contingency Plan Test Report<br>○ Incident Response Plan<br>○ Code Review Report (if applicable)<br>● **Assessment Related Documents**<br>○ Security Assessment Plan (SAP)<br>○ GSA NIST SP 800-53, Revision 5 Test Case Workbook<br>○ Authenticated OS Vulnerability Scan Results<br>○ Authenticated Web Application Vulnerability Scan Results<br>○ Penetration Test Report (if applicable)<br>○ Other Scan Reports, as necessary |

| GSA Subsystem A&A Process |
|---|
| **Authorization Package Documents** |
| ● System Security Plan<br>● Security Assessment Report<br>● Certification Letter<br><br>**Note:** No subsystem ATO Letter or POA&M. The parent system's ATO Letter is updated to list the subsystem. The parent system's POA&M includes any POA&Ms associated with the subsystem. |
| **Other Required Documents (as noted)** |
| ● **ATO Related Documents**<br>○ Privacy Threshold Assessment/Privacy Impact Assessment<br>○ FIPS 199 Security Categorization<br>○ Digital Identity Acceptance Statement<br>○ Interconnection Security Agreement(s)/Information Exchange Agreements (if applicable)<br>○ Control Tailoring Workbook (CTW)<br>○ Code Review Report (if applicable)<br>● **Assessment Related Documents**<br>○ Security Assessment Plan (SAP)<br>○ GSA NIST SP 800-53, Revision 5 Test Case Workbook |

| GSA Subsystem A&A Process |
|---|
| ○ Authenticated OS Vulnerability Scan Results<br>○ Authenticated Web Application Vulnerability Scan Results<br>○ Penetration Test Report (if applicable) |

| GSA Leveraged FedRAMP SaaS Solution Process |
|---|
| **FIPS 199 Low and Moderate Impact SaaS (without PII)** |
| **Authorization Package Documents** |
| ● CRM System Security Plan<br>● Certification Letter<br>● ATO Letter<br>● CRM SAR Attestation<br>● Plan of Action and Milestones |
| **Other Required Documents** |
| ● **ATO Related Documents**<br>○ FIPS 199 Security Categorization<br>○ Privacy Threshold Assessment<br>○ Digital Identity Acceptance Statement<br>● **Assessment Related Documents**<br>○ Annotated CSP CRM and any supporting artifacts |
| **FIPS 199 Moderate Impact SaaS (with PII)** |
| **Authorization Package Documents** |
| ● CRM System Security Plan<br>● Certification Letter<br>● ATO Letter<br>● Security Assessment Report<br>● Plan of Action and Milestones |
| **Other Required Documents** |
| ● **ATO Related Documents**<br>○ FIPS 199 Security Categorization<br>○ Privacy Threshold Assessment/Privacy Impact Assessment<br>○ Digital Identity Acceptance Statement<br>● **Assessment Related Documents**<br>○ Test Cases for CRM controls/requirements |

## Appendix E: Significant Changes - Decision Tree

**Definition:** A Significant change is any modification that materially alters the system's risk posture, authorization boundary, or control effectiveness, requiring AO awareness and potential reauthorization by appropriate system stakeholders.

### Step1: Authorization Boundary

Does this change add, remove, or connect a system, service, or environment outside the currently authorized boundary?

- Yes = Significant Change
- No = Go to Step 2

Examples:

- New external API integration
- New cloud account/subscription
- New SaaS dependency

---

### Step 2: Data & Impact Level

Does this change introduce new data types or increase the system's confidentiality, integrity, or availability impact level?

- Yes = Significant Change
- No = Go to Step 3

Examples:

- Introducing PII, PHI, CUI
- Expanding data retention scope
- Changing encryption or data residency

---

### Step 3: Identity & Access

Does this change modify authentication, authorization, or trust relationships?

- Yes = Significant Change
- No = Go to Step 4

Examples:

- New identity provider
- New admin or privileged roles
- Changes to MFA enforcement

---

### Step 4: Security Controls

Does this change disable, weaken, replace, or bypass an existing security control?

- Yes = Significant Change
- No = Go to Step 5

Examples
- Logging reduced or removed
- Scan gates bypassed
- New CI/CD tools outside approved stack

---

### Step 5: Risk Acceptance

Does this change require acceptance of new or increased risk?

- Yes = Significant Change
- No = Not a Significant Change

Examples:
- Temporary control exceptions
- Compensating controls required
- New unresolved findings

---

### Final Decision

- Any Yes = Significant Change
- All No = Not a Significant Change (covered by existing authorization)

---

### If Significant Change

- Deployment pauses
- Security Impact Analysis (SIA) performed
- ISSO and ISSM engaged
- SecEng (consulted for architecture changes)
- Assessment (Full or Delta) performed

### If Not Significant

- Deployment continues based on routine change management

The final decision and justification must be recorded as evidence in the change management system.