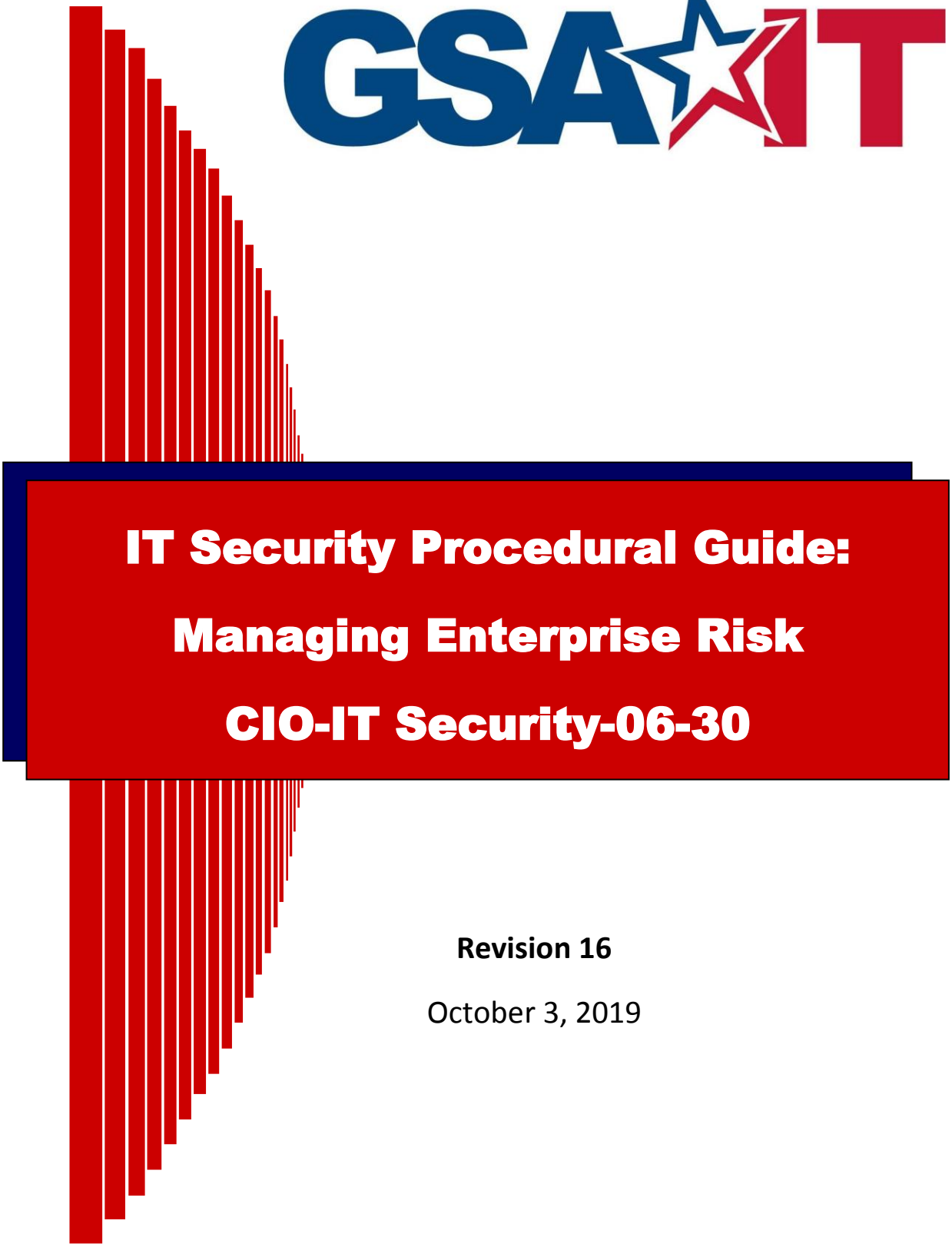

IT Security Procedural Guide: Managing Enterprise Risk CIO-IT Security-06-30

Revision 16

October 3, 2019

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Revision 1 Changes – March 22, 2006				
1	Bo Berlas	Included the OWASP Web Application Penetration Checklist and the OWASP Testing Project documents as embedded objects into Appendix C – GSA Risk Assessment Security Requirements.	To provide a usable checklist for testing the OWASP Top Ten Vulnerabilities.	14
Revision 2 Changes – February 13, 2007				
1	Bo Berlas	Various updates to reflect changes in A&A process	FINAL publishing of NIST 800-53 on 12/2006	4-10
2	Bo Berlas	Updated Appendix A: Risk Assessment Report Format	RA and SA are now combined into a single RA/SA report.	11
3	Bo Berlas	Updated Appendix B: GSA Security Assessment Test Procedures	Updated Assessment test procedures based on FINAL publishing of NIST 800-53 on 12/2006	15
4	Bo Berlas	Updated Appendix C: Plan of Action and Milestone (POA&M) Template	Attached new POA&M template for FY 2007.	16
5	Bo Berlas	Updated Appendix D: Risk Assessment / Security Assessment Plan Template	Updated assessment plan template to reflect combining of RA and SA reports.	17
Revision 3 Changes – March 20, 2007				
1	Bo Berlas	Changed reference to OWASP Top Ten from 2007 Release Candidate 1 back to the 2004 Update.	OWASP Top Ten, 2007 RC1 has not been finalized. GSA will adopt the OWASP Top Ten, 2007 Update upon final publication.	6
2	Bo Berlas	New database scanning requirement.	App Detective or similar tool should be used to test database security configurations.	7
Revision 4 Changes – October 16, 2007				
1	Bo Berlas	Updated policy reference.	GSA IT Security Policy was updated June 2007.	6
2	Bo Berlas	Changed reference to OWASP Top Ten from the 2004 Update to the current 2007 Update.	The 2007 Top Ten lists current web application vulnerabilities.	7
3	Bo Berlas	Replaced the FY 2007 POA&M Reporting Template with the FY 2008 template.	New OMB Quarterly POA&M Reporting Requirements	17
Revision 5 Changes – July 15, 2010				
1	Bo Berlas	Update the A&A process to be consistent with NIST 300-37 and the Risk Management Framework	Updates required to ensure agency compliance.	Various
2	Bo Berlas	Inserted Roles and Responsibilities relating to A&A from the GSA IT Security Policy	Identify A&A Roles and Responsibilities	3
3	Bo Berlas	New implementation guidance for NIST 800-53 controls.	To facilitate implementation of required controls	25

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
4	Bo Berlas	New NIST 800-53 assessment test cases	Required to facilitate assessment of NIST 800-53 controls	Appendix C
5	Bo Berlas	New OCISO A&A Review SOP	Documents the process for submission of A&A packages to the OCISO and the detailed procedural steps performed by the OCISO to verify A&A compliance.	Appendix E
6	Bo Berlas	New guidance for A&A of Minor Systems	To facilitate assessment of minor systems.	22
Revision 6 Changes – December 16, 2010				
1	Bo Berlas	Updated references for Certification, Accreditation, and Certification and Accreditation (C&A) to Assessment, Authorization, and Assessment and Authorization (A&A), respectively.	To be consistent with the current terminology in NIST 800-37.	Throughout
2	Bo Berlas	Inserted guidance for forming sections 1-10 of the SSP for cloud computing system SSPs.	To address cloud specific security challenges.	12
Revision 7 Changes – May 31, 2011				
1	Bo Berlas	Updated references to A&A to security authorization process and authorization package or A&A package to security authorization package.	To be consistent with the current terminology in NIST 800-37.	Throughout
2	Bo Berlas	Inserted guidance for review of minimal impact SaaS solutions.	To document required review activities for such systems.	25
3	Bo Berlas	Updated Appendix E to include a revised OCISO Security Authorization Package Review SOP.	To reflect current version of the SOP.	48
Revision 8 Changes – November 25, 2015				
1	Lewis/ Sitcharing	Changes made throughout the document to reflect NIST and GSA requirements	Updated to reflect and implement the most current NIST 800-53-Rev4 and GSA requirements	Various
Revision 9 Changes – May 19, 2016				
1	Wilson/ Klemens	Restructuring of the document, modifications to specific process descriptions.	Updated to reflect current acceptance of risk process and rename Minor Application process to Subsystem process and revise its description. Restructuring and editing throughout.	Various
Revision 10 Changes – April 10, 2017				
1	Desai/ Klemens	Clarifying system definitions and penetration testing requirements.	Included definitions of Federal and Contractor systems. Clarified when systems are required to have penetration tests as part of their assessment.	Sections 1.2, 4.1.7
2	Klemens	Update and edit document.	Updating of hyperlinks, editing of document, updates to align with other GSA documents.	Throughout
Revision 11 Changes – October 10, 2017				

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
1	Dean/ Feliksa/ Klemens	Update hyperlinks and minor editorial changes.	Hyperlinks were updated so outdated, superseded documents would not be provided. Minor edits to clarify current GSA processes.	Throughout
Revision 12 Changes – January 17, 2018				
1	Feliksa/ Klemens	Integrate the NIST Cybersecurity Framework (CSF), update A&A process and POA&M information, remove Cloud Controls.	Comply with Executive Order 13800, update processes based on revised procedures, streamline document by moving cloud controls.	Throughout
Revision 13 Changes – May 14, 2018				
1	Klemens	Added a provision for piloting new A&A processes. Updated Lightweight Security Authorization Process, MiSaaS, CSF content.	Allows a new A&A process to be piloted/tested. Align with revised GSA and NIST guidance.	Sections 1, 3.2.2, 3.2.6, Appendix A, Appendix C
Revision 14 Changes – February 1, 2019				
1	Klemens	Updated information on compliance/configuration scans. Updated hyperlink references. Added Program and Project Manager roles. Removed CTW as attachment to SSP.	Clarify GSA policy and guidance on compliance to hardening guides. Update to new format and style for hyperlinks. Added roles added to 2100.1. Data in the CTW is available in the SSP Template and Control Summary Table.	Throughout
2	Klemens	Added information concerning Binding Operational Directives (BOD) requirements and clarified encryption of data at rest requirements.	Clarify GSA policy and guidance on BOD and encryption requirements.	10, 12, 14, 38, 47
3	Klemens	Updated penetration testing requirements. Editing to align with current format, style, structure.	Provide the latest guidance on penetration testing requirements	34, 38, various
Revision 15 Changes – July 25, 2019				
1	Klemens	Updated SC-28 (1) control applicability and parameter. Revised references to Binding Operational Directives (BODs) to Cybersecurity Directives which include BODs and Emergency Directives. Revised parameter for SI-2(3).	Updated GSA parameters and guidance on NIST controls.	Multiple
Revision 16 Changes – October 3, 2019				
1	Dean/ Klemens	Revised to include/update information on Showstopper Controls, configuration compliance metric, vulnerability remediation timeframes, reference additional procedural guides, and add Certification Letter as part of security authorization process.	Updated to reflect additional Federal and GSA guidance and process changes.	Multiple

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
2	Klemens	Added PL-8 and SA-8 to the table of GSA required controls, removed LATO SSP/SAR/Test Cases from LATO process description and appendices.	Updated to reflect additional Federal and GSA guidance and process changes.	Multiple

Approval

IT Security Procedural Guide: Managing Enterprise Risk, CIO-IT Security-06-30, Revision 16, is hereby approved for distribution.

X DocuSigned by:
Bo Berlas
EE97B6D7B34D4DF...

Bo Berlas
GSA Chief Information Security Officer

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

Table of Contents

Table of Figures and Tables

NOTE: Hyperlinks in this guide are provided as follows:

- Appendix B - Consolidated List of Guidance, Policies, Procedures, and Forms. This appendix contains hyperlinks to Federal Regulations/Guidance and to GSA webpages 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 webpage or document listed in Appendix B. For example, Google Forms, Google Docs, and websites will have links.

Note: It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

1 Introduction

Security Assessment and Authorization (A&A) processes within the General Services Administration (GSA) 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 risk through a system life cycle perspective including system security authorization and continuous monitoring. It is designed to assist agency and contractor personnel with security responsibilities in implementing A&A processes.

Every GSA Information Technology (IT) system must use one of the A&A processes identified in this guide or a pilot process as described in the next paragraph. 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 Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and authorized by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form.

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 Authorization to Operate (ATO) resulting from the pilot.

Executive Order (EO), EO 13800, "*Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"* requires all agencies to use "The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the NIST or any successor document to manage the agency's cybersecurity risk." This NIST document is commonly referred to as the Cybersecurity Framework (CSF). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's RMF as its foundation for managing risk. Further information on how the CSF relates to GSA's use of the NIST RMF is explained in Section 2 and Appendix A where the CSF categories and subcategories are mapped to NIST RMF steps, tasks, and security controls.

In Appendix F, Table F-1, GSA has identified a list of NIST SP 800-53 controls considered to be Showstopper Controls. Showstopper controls, if not fully compliant, will keep a system from receiving a full ATO.

1.1 Purpose

This procedural guide defines the GSA risk management process, specifically the security authorization processes GSA has implemented for information systems to obtain an ATO. The guide describes the key activities in managing enterprise-level risk as described in NIST SP 800-37.

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, the specific processes to follow for properly accomplishing A&A activities for the systems under their purview. The following definitions are provided for classifying systems within scope of this guide.

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

1.3 Policy

As detailed within CIO 2100.1, Authorizing Officials (AO) 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 at least every three (3) years unless it is covered by GSA's Information Security Continuous Monitoring (ISCM) program.

1.4 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/Staff Office (S/SO) 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 Chapter 2 of CIO 2100.1. The following sections provide a high level description of the responsibility for the primary roles with management and operational A&A responsibilities.

1.4.1 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.

1.4.2 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.

1.4.3 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 Chief Information Security Officer (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.

1.4.4 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 controls in Appendix J: Privacy Control Catalog of NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*". Within GSA, the CIO has designated the Deputy CIO as the SAOP.

1.4.5 GSA Chief Privacy Officer (CPO)

The CPO is responsible for overseeing GSA's Privacy Program whose mission it 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.

1.4.6 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.

1.4.7 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.

1.4.8 Office of CISO Division Directors

OCISO Directors are the intermediary to the AO for ensuring IT security is properly implemented. The Director is the focal point for all IT system security matters for the IT resources under their responsibility.

1.4.9 Information Systems Security Managers (ISSMs)

ISSMs report to the ISSO Support Division (IST) 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 are appointed, in writing, by the Director of IST 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.

1.4.10 Information Systems Security Officers (ISSOs)

ISSOs are responsible for ensuring implementation of adequate system security, including privacy analysis/protection, in order to manage cybersecurity risk aligned with the 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.

1.4.11 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.

1.4.12 Program Managers

Program Managers are management officials within GSA who are responsible for developing, implementing, and/or overseeing multi-year IT initiatives that must be carried out through multiple related projects. A Program Manager focuses on the strategic goals of GSA. Program Managers are responsible for ensuring cyber risk is adequately managed and resources are allocated, monitored, and managed to support the required level of security for projects under their purview.

1.4.13 Project Managers

Project Managers are management officials within GSA who are responsible for managing a project within a larger program. A Project Manager is responsible for ensuring cyber risk is adequately managed and the schedule, resources, and tasks within a project include delivering security.

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

Data Owners are responsible for determining the security categorization level of systems based upon Federal Information Processing Standards (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.

1.4.15 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.

1.4.16 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.

1.4.17 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.

1.4.18 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.

2 GSA Standard A&A Process

All GSA A&A processes are based upon NIST SP 800-37. A depiction of the RMF is provided in Figure 2-1.

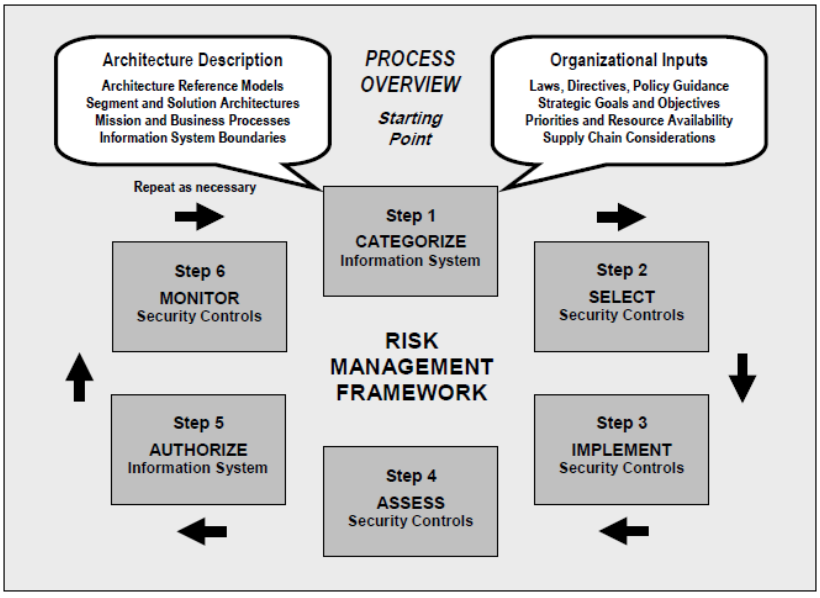

Figure 2-1. Risk Management Framework (from NIST 800-37)

Note: This guide will be updated to incorporate NIST SP 800-37, Revision 2 in the near future.

The RMF Steps 1-6 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 3 which have been adapted or modified from the standard RMF processes. Documents required as part of a GSA A&A process are listed in Appendix C along with hyperlinks (where applicable) to resources containing document templates.

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

- **Identify (ID):** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect (PR):** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect (DE):** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond (RS):** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover (RC):** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

GSA's alignment of its implementation of the NIST RMF with these five core functions is portrayed in Table 2-2. The mapping was based on reviewing NIST's mapping in the draft version of Revision 2 to NIST SP 800-37 and how GSA manages risk across the enterprise. A more detailed mapping of the CSF Functions, Categories, and Subcategories to NIST SP 800-53 security controls is provided in Appendix A.

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

CSF Function	Mapped RMF Steps
Identify	RMF Step 1: Categorize Information System Task 1-1: Security Categorization Task 1-2: Information System Description Task 1-3: Information System Registration RMF Step 2: Select Security Controls Task 2-1: Common Control Identification Task 2-2: Security Control Selection
Protect	RMF Step 2: Select Security Controls Task 2-2: Security Control Selection Task 2-3: Monitoring Strategy RMF Step 3: Implement Security Controls Task 3-1: Security Control Implementation
Detect	RMF Step 3: Implement Security Controls Task 3-1: Security Control Implementation RMF Step 4: Assess Security Controls Task 4-2: Security Control Assessment

CSF Function	Mapped RMF Steps
	RMF Step 6 Monitor Security Controls Task 6-2: Ongoing Security Control Assessments Task 6-5: Security Status Reporting
Respond	RMF Step 3: Implement Security Controls Task 3-1: Security Control Implementation RMF Step 4: Assess Security Controls Task 4-4: Remediation Actions RMF Step 5: Authorize Information System Task 5-1: Plan of Action and Milestones Task 5-4: Risk Acceptance RMF Step 6 Monitor Security Controls Task 6-3: Ongoing Remediation Actions Task 6-5: Security Status Reporting
Recover	RMF Step 3: Implement Security Controls Task 3-1: Security Control Implementation RMF Step 4: Assess Security Controls Task 4-4: Remediation Actions RMF Step 5: Authorize Information System Task 5-1: Plan of Action and Milestones RMF Step 6: Monitor Security Controls Task 6-3: Ongoing Remediation Actions Task 6-6: Ongoing Risk Determination and Acceptance

2.1 RMF Step 1 – Categorize Information System

The first step in GSA's standard A&A process is to determine the FIPS 199 security categorization level of the information system. This level (Low-, Moderate-, or High-impact) will affect the remaining steps in the process. The following tasks detail the actions in RMF Step 1.

TASK 1-1: Security Categorization - Categorize the information system using the FIPS 199 Security Categorization Template and document the results of the security categorization in the system security plan (SSP). The System Owner carries out the security categorization process in cooperation and collaboration with appropriate organizational officials with information security/risk management responsibilities including but not limited to the Data Owner, AO, ISSM, and ISSO. The process for determining the appropriate impact level is outlined in FIPS 199 and its associated guides:

- 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.*"

Please refer to these documents to categorize the information system. The resulting categorization determines the appropriate security control baseline (Low-, Moderate-, or High-

impact) for the information system as outlined within NIST SP 800-53, Revision 4. The baseline is refined in the GSA Control Tailoring Workbook (CTW) to meet GSA's specific needs regarding assignment parameters and applicability of controls.

NOTE: Since forms, templates, and guides are updated frequently, always visit the IT Security Forms and IT Security Procedural Guides pages to ensure the most current version of templates and guides are used.

TASK 1-2: Information System Description - Describe the information system (including system boundary) and document the description in an SSP based on NIST SP 800-18, Revision 1, "*Guide for Developing Security Plans for Federal Information Systems.*" The SSP provides an overview of the security requirements for the information system, describes the security controls in place or planned for meeting those requirements, and formalizes the plans and expectations regarding the overall functionality of the information system. Descriptive information about the information system is documented in sections 1-12 of the security plan. The level of detail provided in the security plan should be commensurate with the security categorization of the information system. The following sections should be sufficiently detailed:

- Section 2 of the SSP describes the FIPS 199 security categorization of the system. The FIPS 199/NIST SP 800-60 analysis must be supported by a completed FIPS 199 Security Categorization Template.
- Section 9 of the SSP describes the function or purpose of the system and its information processes.
- Section 10 of the SSP contains tables outlining the technical system including an inventory of all assets in the authorization boundary. The tables within this section must be completed and depict a complete inventory of hardware, software and operating system components. Any subsystems included as a part of the system must be separately identified in Appendix C to the SSP, this appendix will be included as an attachment to the system's ATO Letter.
- Section 11 of the SSP must list all interconnections including the system name, organization, system type; indicate if there is an Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA) on file, date of agreement to interconnect, FIPS 199 security category, ATO status, and the name of the AO. Per GSA IT Security Policy 2100.1, "All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be documented in ISA that is approved by the AOs and concurred by the GSA CISO.*"* Per NIST 800-47, *"Security Guide for Interconnecting Information Technology Systems"* an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc."

Contact the OCISO at ispcompliance@gsa.gov with questions or requests for further clarification.

TASK 1-3: Information System Registration - Register the information system with the appropriate organizational program/management offices and security personnel. Inform the OCISO, the System/Application ISSM, and, if different, the ISSM of the larger system on which the system will reside and from which it will inherit security controls. In addition, each IT system is also an IT investment, which needs to be associated with a Unique Investment Identifier.

2.2 RMF Step 2 – Select Security Controls

Based on the FIPS 199 impact level (Low-, Moderate-, or High-impact) determined in Step 1, the appropriate controls will be selected based on GSA's CTW which also provides the assignment parameters for the applicable NIST SP 800-53 controls. In RMF Step 2, controls will be identified as system-specific, hybrid, or common; controls will be tailored and supplemented (as necessary) with additional controls and/or control enhancements to address unique organizational or system specific risks; a monitoring strategy will be developed; and the AO's, or designated representative's, approval of the SSP obtained.

The following tasks detail the actions in RMF Step 2.

TASK 2-1: Common Control Identification – Leverage GSA-IT Security-18-90, "*Information Security Program Plan (ISPP)*," to identify the GSA common controls and document them in the SSP initiated in RMF Step 1. Common controls are security controls that are inherited. Common control sources may include the OCISO, GSA enterprise systems, S/SO systems, and other sources. System Owners inheriting common controls can either document the implementation of the controls in their respective security plans or reference the controls contained in the security plans of the common control providers.

Common control providers are responsible for:

- documenting common controls in a security plan (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 plan of action and milestones 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 Plan of Action and Milestones (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 Summary Table pertaining to the FIPS 199 impact level associated with the system must be completed. The table identifies control types (common vs. hybrid controls vs. system specific controls) with implementation status (Fully Implemented, Partially Implemented, Planned, etc.) across required controls. The table should be customized to the GSA S/SO or contractor's environment to account for common controls and subsystems (as necessary). Control Summary Table templates are available for use on the IT Security Forms page (search for "summary" on the web page to ensure the latest summary table is used).

The completed Control Summary table will be included in the appendices section of 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.

TASK 2-2: Security Control Selection - Select the security controls for the information system and document the controls in the SSP. The security controls are selected based on the FIPS 199 security categorization determined in RMF Step 1, Task 1-1, forming the minimum security control baseline for the information system. Once the security control baseline is determined, it must be tailored by applying scoping, parameterization, compensating control guidance, and any GSA required controls. The tailored baselines, as necessary, can be supplemented with additional controls and/or control enhancements to address unique organizational and/or system specific needs based on a risk assessment (either formal or informal) and local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.

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 will be documented in the SSP. Define the settings deferred to S/SO or contractor recommendation to be reviewed and accepted by the GSA AO.

Note: Additional Federal requirements such as DHS Cybersecurity Directives must be included in a system's set of requirements when the system contains components to which they apply.

TASK 2-3: Monitoring Strategy - Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation. The developed strategy may follow the RMF Step 6 - Security Control Monitoring process outlined within Section 2.6.1 of this guide, or the process in CIO-IT Security-12-66, "*Information Security Continuous Monitoring Strategy*" for systems in GSA's Continuous Monitoring Program. The Information System Continuous Monitoring Plan Template described in CIO-IT Security-12-66 may be used by any System Owner to help form an initial strategy.

TASK 2-4: Security Plan Approval - Review and approve the security plan. The System Owner shall submit the SSP with the following appendices/attachments to the ISSO, ISSM, and the AO. The remainder of the SSP's appendices and attachments will be completed as the security controls are implemented in RMF Step 3.

- Appendix A - Acronyms, Terms, and Definitions
- Appendix B - References
- Appendix C - Hosted Subsystems (if applicable)
- Attachment 1: Privacy Threshold Analysis/Privacy Impact Assessment
- Attachment 2: FIPS 199 Security Categorization
- Attachment 3: Digital Identity Acceptance Statement (if applicable)
- Attachment 4: Interconnection Security Agreement (if applicable)
- Attachment 5: GSA Control Summary Table
- Attachment 6: Contingency Plan
- Attachment 7: Contingency Plan Test Report
- Attachment 8: Incident Response Plan
- Attachment 9: Incident Response Plan Test Report
- Attachment 10: Configuration Management Plan (FIPS 199 Moderate and High only)
- Attachment 11: Continuous Monitoring Plan (if applicable)
- Attachment 12: Rules of Behavior (if applicable)
- Attachment 13: Code Review Report (if applicable)

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

The OCISO will review the SSP to determine if it is complete, consistent, and addresses the security requirements for the information system. Based on the results of the review, the SSP may require further updating, or may be approved. The AO or designated AO representative, by approving the security plan, agrees to the set of security controls (system-specific, hybrid, and/or common controls) proposed to meet the security requirements for the information system; allowing Step 3 of the RMF to begin.

- The Security Engineering Division (ISE) in the OCISO must review and approve the Security Architecture before the system's security controls are implemented.
- Security Plans will be submitted by the System Owner/Program Manager through the ISSO and ISSM to the Director of IST for review.
- The OCISO Director of IST must accept the SSP before security control implementation activities can begin.

2.3 RMF Step 3 – Implement Security Controls

Following the approval of the SSP received in RMF Step 2, implement the security controls specified in the SSP.

The following tasks detail the actions in RMF Step 3.

TASK 3-1: Security Control Implementation - 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.

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

TASK 3-2: Security Control Documentation - Describe the security control implementation in the SSP, providing a functional description of how the control is satisfied. The security control implementation descriptions should include planned inputs, expected behavior, 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 are documented in Section 13 of the SSP. This section must provide a thorough description of how the NIST SP 800-53 security controls for the system are being implemented or planned to be implemented. For each control, descriptions must include:

- the security control title;
- how the security control is being implemented or planned to be implemented;
- any scoping guidance that has been applied and what type of consideration;
- identify the control type (Common, Hybrid, System Specific); and
- identify the implementation status (Implemented, Partially Implemented, Planned, N/A, Alternate Implementation, etc.), and who is responsible for its implementation.

Note: Systems with multiple components or subsystems must describe control implementations across all components.

2.4 RMF Step 4 – Assess Security Controls

Upon implementation of security controls in RMF Step 3, perform a security control assessment to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Complete the tasks below to determine in place security controls, prepare a SAR, and initiate corrective actions based on the findings and recommendations within it.

The following tasks detail the actions in RMF Step 4.

TASK 4-1: Assessment Preparation - Develop, review, and obtain approval for a Security Assessment Plan (SAP) which will be leveraged to assess the security controls of the information 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 4-2. Review, update, and/or supplement GSA's NIST 800-53 Rev 4 Test Cases. Add additional assessment test cases for any supplemented controls and/or control enhancements added during Task 2-2, Security Control Selection, to address unique organizational and/or system specific needs.

Note: Assessment of additional Federal requirements including, but not limited to, DHS Cybersecurity Directives (i.e., Binding Operational Directives and Emergency Directives) must be included in the SAP as appropriate.

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

- **FIPS 199 Moderate** and **High** impact systems must be assessed by an independent third party. The use of an independent assessment team reduces the potential for impartiality or 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** information 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. Where a GSA benchmark exists, configuration scanning must be to 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** information systems with web servers must conduct an authenticated vulnerability scan for the most current Open Web Application Security Project (OWASP) Top Ten Most Critical Web Applications Security Vulnerabilities. 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** information systems with database servers must have their databases assessed as part of their OS vulnerability scanning.
- **All Internet accessible systems, FIPS 199 High impact level, and High Value Asset (HVA)** information 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 Assessment and Authorization (A&A) package.

- **All FIPS 199 impact level** information systems are encouraged (and required per the Lightweight and MiSaaS A&A processes) by GSA OCISO to conduct a code analysis using tools to examine the software for common flaws and document results in a Code Review Report per NIST SP 800-53 Control SA-11 enhancement (1).

Note: The 06-30 Scanning Parameter Spreadsheet contains a listing of scanning frequency by technology type and A&A process.

The SAP must be reviewed and approved by the System Owner, ISSO, and ISSM to ensure that 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
- outlines automation to support the concept of continuous monitoring and near real-time risk management.

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

TASK 4-2: Security Control Assessment - Assess the security controls following the SAP and using the NIST 800-53 Rev 4 Test Cases, including any supplemental or updated tests based on the specific system as identified in Task 4-1 (e.g., assessing BODs or other Federal requirements). The assessment determines if the controls implemented in RMF Step 3 are operating as intended and producing the desired outcome with respect to meeting the security requirements for the information system.

TASK 4-3: Security Assessment Report (SAR) - Prepare a Security Assessment Report documenting the issues, findings, and recommendations of the security control assessment (including, if applicable, a penetration test report as an attachment). Document the assessment findings with recommendation(s) and risk determinations from the NIST SP 800-30 Revision 2, *"Guide for Conducting Risk Assessments."* Note that this revision of NIST 800-30 expands the risk rating matrix to five levels; Very Low, Low, Moderate, High, and Very High (equivalent to Critical). Findings in the SAR will be addressed in the following manner:

Findings from Test Cases. Each individual finding must be assessed for risk.

Note: Any additional findings based on Federal requirements, such as BODs, must be reported in the SAR.

Findings from Vulnerability Scans. Individual findings must be identified; however, findings may be grouped and assessed by level and type of scan. These findings should be assessed in the following groupings and associated with NIST SP 800-53 control SI-2.

1. Very High (Critical)/High OS (includes DB, if applicable) Findings
2. Very High (Critical)/High Web Application Findings
3. Moderate OS (includes DB, if applicable) Findings
4. Moderate Web Application Findings

Low risk findings based on scans do not have to be assessed within the SAR; however, those findings need to be included in the scan results attached to the SAR.

Findings from Configuration/Compliance Scans. Individual findings must be identified. The findings will be discussed as one group. It will be listed at the Moderate level and associated with NIST SP 800-53 control CM-6.

Risk must be determined for findings, as described above, and an overall system or application risk determined. The risk determination will be included as part of the authorization package. Refer to NIST SP 800-30, Revision 2 to ensure that all necessary risk assessment areas are completed.

The risk assessment should consist of the following steps:

- Identifying 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;
- Aligning threat sources and events with vulnerabilities;
- Assessing each system instance of absent controls and/or vulnerabilities identified during the security assessment. Evaluate the likelihood the threat sources and events will exploit an 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, and;
- Evaluate the risks of all identified vulnerabilities to determine an overall level of risk for the system or application.

The SAR must document all findings from the security assessment test cases that are not FULLY SATISFIED and address scan findings as described above. Assessments must include vulnerabilities, threats, an in place controls discussion, likelihood, impact, risk discussion/rating, and recommendations for correcting deficiencies in security controls. Assessment results for subsystems, if any, should be included as a subsection to Section 6 – Findings Discussion of the hosting system's SAR. If there is more than one subsystem, a separate subsection should be created for each subsystem.

Note: Review and consider ALL risk categories in the process of preparing the final SAR. It is a common mistake to ignore some classes since they are incorrectly believed to be "low risk". However all scanner tools can categorize findings, in much the same way that false positive findings are not real issues, false negative findings or "low/info risk" findings can be real issues, which a human reader will understand are necessarily 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 level systems can possess Very High (Critical)/High risk findings the same as FIPS 199 High level systems.

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

2.5 RMF Step 5 – Authorize Information System

Following assessment of the information system in RMF Step 4, the POA&M is prepared (updated if an existing system with a POA&M) based upon the results of the security assessment and any remedial action to correct findings; the Security Authorization Package is assembled and submitted to the AO for adjudication. The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the overall risk to the agency is acceptable.

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

The following tasks detail the actions in RMF Step 5 – Authorize Information System.

TASK 5-1: Plan of Action and Milestones - Prepare the POA&M from the findings and recommendations in the SAR excluding any remediation actions taken.

Develop the POA&M as follows:

- Do not include vulnerabilities identified as ‘‘Resolved” in the SAR.
- Include any vulnerabilities associated with End-of-Life (EOL) software, regardless of the associated risk level.
- Do not include vulnerabilities identified as Low/Very Low risk in a POA&M, unless they are associated with EOL software or audit findings. Low/Very Low vulnerabilities still need to be included in the SAR either in relation to a NIST control test case or in the scan results appendices/attachments.
- Very High (Critical), High, and Moderate risk vulnerabilities need to be included in the POA&M using the following criteria:
    - Assessment findings from test cases become individual entries in the POA&M.

- Findings based on scans are grouped based on the type of scan (i.e., OS, Web Application).
  - Vulnerability Scans. Findings will result in one POA&M entry (per scan type-e.g., OS, Web Application) covering all Very High (Critical)/High and Moderate findings on all assets within the FISMA system boundary. Vulnerability scan POA&Ms will state):

    "Vulnerability scans have identified vulnerabilities for the system. Critical/Very High vulnerabilities for Internet-accessible IP addresses must be remediated within 15 days, for all other assets Critical/Very High vulnerabilities must be remediated within 30 days; High vulnerabilities must be remediated within 30 days; Moderate vulnerabilities must be remediated within 90 days."

  - Configuration/Compliance Scans. A FISMA system must monitor compliance to all of the configuration settings required by GSA hardening guides. Each configuration setting must be covered by one of the following clauses:
    - The configuration setting is compliant - The asset's setting is either
      - Equal to the setting required, or
      - More restrictive than the setting required.
    - The configuration setting is not compliant - The asset is configured with a more liberal setting than required. In this case, the non-compliant configuration setting needs to be accounted for in one of the following ways:
      - Deviation - The non-compliant setting is covered by an approved deviation.
      - POA&M - If the composite compliance percentage of all assets with a single operating system is below 85% for over 90 days, a POA&M must be created for the non-compliant operating system. The resultant POA&M will state:

        "Configuration/compliance scans indicate at least one operating system within the FISMA system boundary has been below 85% compliant for over 90 days."

Note: GSA systems not being scanned under GSA's vulnerability scanning program must include all identified weaknesses in their POA&Ms in order to provide GSA OCISO visibility into their vulnerabilities. Vulnerabilities can be individually reported or grouped together and presented by risk level with each grouping constituting an explicit entry in the POA&M (e.g., FYXX Q1 High Risk Scan Findings – 2 vulnerabilities, or FYXX Q1 Moderate Risk Scan Findings – 5 vulnerabilities). Supporting scan reports must be provided to the OCISO ISP division as part of updating the POA&M via the POA&M Google Team Drives. Scan folders are located inside of appropriate system Team Drives.

The POA&M describes how the System Owner intends to address vulnerabilities (i.e., reduce, eliminate, or mitigate vulnerabilities). A POA&M Template and details on developing POA&Ms are contained in the POA&M procedural guide and on the POA&M Guidance Team Drive. A GSA POA&M Template may be obtained by contacting ispcompliance@gsa.gov. For every Open or Outstanding finding in the SAR (as described above), there must be a related planned action in the POA&M for the associated NIST SP 800-53 control or enhancement.

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

TASK 5-2: Security Authorization Package – The ISSO assembles the security authorization package. 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. The documentation required and links to document templates for other A&A processes GSA uses (and the standard process) are listed in Appendix C.

TASK 5-3: Risk Determination - If an adequate level of information is provided to establish a creditable level of risk, the AO will make a risk level determination. For this determination, the AO assesses all of the information provided by the System Owner as 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.

TASK 5-4: Risk Acceptance – The explicit acceptance of risk is the responsibility of the AO. The AO determines if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable. The AO must consider many factors, balancing security considerations with mission and operational needs. The AO issues an authorization decision for the information system and the common controls inherited by the system after reviewing all of the relevant information. The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the risk to the agency is acceptable. Following review of the security authorization package and consultation with key agency officials, the AO must render an authorization decision. As noted in the following section, the CISO concurs/non-concurs with the residual risk being accepted as part of the ATO process.

A&A Package Review & Approval. The process for reviewing A&A packages for the GSA standard A&A process is as follows.

The ISSO with assistance from the System Owner assembles the security authorization package (including certification and ATO letters), signs the certification letter, and submits the package to the ISSM for review. The ISSM will review the package, requesting the ISSO address any inconsistencies/issues. Once satisfied with the package, the ISSM signs the certification letter, and forwards the package to the OCISO IST Director.

The OCISO IST Director will review the package to provide assurance to S/SO AOs that the systems for which they are responsible have followed required Federal and GSA policy and procedures. Upon completion of this review, the OCISO IST Director signs the certification letter recommending concurrence to the CISO and forwards the package the CISO. Non-concurrences are sent back to the ISSM to address any inconsistencies/issues.

The CISO considers the IST Director's recommendation, collaborates with the AO and others, as necessary, and concurs or non-concurs with granting an ATO prior to submitting the package to the AO. Concurrences are forwarded to the AO, non-concurrences are returned to the OCISO IST Director.

The AO reviews the security authorization package. Based on a determination of the documentation and supporting evidence and whether it establishes an acceptable level of risk the AO may:

- Authorize system operation w/out 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 full ATO without any restrictions/limitations; or
- Not authorize the system for operation.

Note: The System Owner/ISSO must update the SSP and POA&M to reflect any conditions set forth in the Certification and/or ATO letters. The updated security authorization package including the Certification and ATO letter must be uploaded into the GSA Archer A&A Repository and copies distributed to the ISSO, ISSM, and System Owner. An email must be sent to the OCISO at ispcompliance@gsa.gov indicating the package has been uploaded into the A&A Repository.

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

- Embedded software dependencies
- COTS product update time lines

- Compatibility issues between components

AORs are not intended for delayed or ineffective flaw remediation processes (i.e., patching), insufficient out-year System Development Life Cycle planning (for legacy components), or System Owner preferences. 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. AOR letters have a maximum duration of one year. Upon expiration a new AOR letter may be requested, however it must include new details as to why the vulnerabilities must remain unresolved. AOR letters received without such additional detail will not be approved. Based on the criteria above, AOR letters are:

- Not required for Very Low/Low risk vulnerabilities and findings.
- Required for Moderate risk vulnerabilities and findings. Moderate risk AOR letters require AO approval, but not CISO concurrence.
- Required for Critical/Very High/High risk vulnerabilities and findings. Critical/Very High/High risk AOR letters require AO approval and CISO concurrence.

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

1. System Owner/Custodian, ISSO, and ISSM determine the need for an AOR letter based on system POA&Ms.
2. ISSO in conjunction with the ISSM prepares the AOR letter, ensuring an AOR number is added to the footer of the letter.
3. Director of IST notifies the CISO if review and discussions with all stakeholders is appropriate.
4. ISSM submits letter and recommendation to:
   a. AO for approval for Moderate risk vulnerabilities
   b. AO for approval and CISO concurrence for Critical/Very High/High vulnerabilities.
5. Approved AOR letters become part of the permanent A&A file maintained by the ISSO and ISSM. AOR letters must be uploaded into the Archer A&A Repository and an email sent to ispcompliance@gsa.gov indicating an AOR letter has been uploaded.
6. The ISSO is responsible for monitoring POA&Ms and AOR letters. After one year:
   a. If POA&Ms listed in the AOR letter are still unresolved, a new AOR letter is required with additional details on why the vulnerabilities/findings are unresolved.
   b. If all POA&Ms have been resolved, then the AOR letter is noted as completed and archived as a historical record of the system's A&A status.

A&A Repository. Upon obtaining a signed ATO Letter, the ISSO will upload a copy of all A&A documentation into the Archer A&A Repository.

2.6 RMF Step 6 – Security Control Monitoring

2.6.1 Security Control Monitoring

TASK 6-1: Information 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*," GSA has a rigorous configuration change management process. The strategy states that IT changes are 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 tested and validated prior to implementation into the production environment. Configuration settings and configuration baselines are updated as necessary to meet new technical and/or security requirements and are controlled through the CM process.

TASK 6-2: Ongoing Security Control Assessments – System Owners are responsible for assessing a subset of the NIST SP 800-53 security controls employed within and inherited by the information system in accordance with GSA's monitoring strategy. Per CIO-IT 01-05, the implemented CM process calls for continuous system monitoring to ensure that systems are operating as intended and that implemented changes do not adversely impact either the performance or security posture of the systems. Per CIO-IT Security-18-91, GSA's annual FISMA self-assessments will assess a subset of security controls, common controls that have been identified as weaknesses for GSA systems in past assessments, and other key controls that GSA has identified. Penetration testing and OIG audits may also be performed for a few selected systems as part of an annual assessment.

TASK 6-3: Ongoing Remediation Actions – 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 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 mitigation shall be the appropriate risk response for all critical/very high and high risks vulnerabilities that can be exploited from the Internet and cannot be accepted, avoided, shared, or transferred. Critical/Very High vulnerabilities for Internet-accessible IP addresses must be remediated within 15 days, for all other assets Critical/Very High vulnerabilities must be remediated within 30 days; High vulnerabilities must be remediated within 30 days; Moderate vulnerabilities must be remediated within 90 days, and low/very low risk vulnerabilities will be addressed on a case-by-

case basis. 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.

TASK 6-4: Key Updates – The System Owner and ISSO will update the following items as part of the system and GSA continuing 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
- Annual penetration tests
- Audits, or related assessments
- Changes identified as part of a system's Configuration Management (CM) Plan
- Changes identified as part of a system's Information Security Continuous Monitoring Plan, for systems with 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.

TASK 6-5: Security Status Reporting - The System Owner and ISSO will report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the AO and other appropriate organizational officials on an ongoing basis. GSA's vulnerability management program, the GSA POA&M management process, and any required reporting programs will be used to provide security status reporting. AOs and other personnel with security related responsibilities will leverage these resources to keep apprised of the risk levels associated with their system(s).

TASK 6-6: Ongoing Risk Determination and Acceptance – The System Owner, AO, and ISSO will review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis. In accordance with GSA's continuous monitoring strategy and the system's continuous monitoring plan the review will determine whether the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation (where applicable) remains acceptable. Data reported via GSA's vulnerability scanning program, the GSA POA&M management process, annual assessments, and other assessment processes (e.g., Penetration Testing, audits, and

FISMA metrics) will be used by the AO to determine the acceptance of risks and the need to perform reauthorization.

TASK 6-7: Information System Removal and Disposal – System Owners and ISSOs will establish a disposal plan in accordance with NIST SP 800-64, Revision 2, "*Security Considerations in the Information System Development Life Cycle*", CIO Order 2140.4, and "*Information Technology (IT) Solutions Life Cycle (SLC) Policy*". In support of this plan, 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, and CIO-IT Security-06-32, "*Media Protection (MP)*".

2.6.2 Information Security Continuous Monitoring Strategy

Inventoried GSA systems that have attained an ATO may request entrance into GSA's Information Security Continuous Monitoring (ISCM) Program. Systems that meet the qualifying requirements of this program no longer follow the standard security authorization process for GSA information systems. New systems must follow one of the GSA A&A processes to obtain an ATO, including re-authorization prior to its ATO expiration, when the system undergoes a significant change, or when there is a major security breach impacting the security posture of the system. Specific requirements for admittance into the ISCM Program are detailed in CIO-IT Security-12-66.

2.6.3 Security Authorization Process Guidance for Significant Changes

Significant changes as defined in NIST SP 800-37, Appendix F, require reauthorization following the security authorization process requirements in this guide. Contact the OCISO at ispcompliance@gsa.gov to determine the scope of reauthorization activities.

2.6.4 Security Authorization Process Guidance for Expiring Authorizations

ISSOs with assistance from the ISP Division can track the expiration dates of ATOs. Renewal of ATOs are initiated by the Authorizing Officials, ISSMs and ISSOs. Per Chapter 3 of GSA CIO 2100.1:

l. 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 (e.g., System Security Plan, Contingency Plan, POA&Ms). All actions to satisfy the conditions below must be completed within the extension period (i.e., no longer than 12 months).

(1) Transitioning to ongoing authorization;
(2) Planning for disposal;
(3) Consolidating into another system for its ATO. The scope of consolidation shall be approved by the OCISO prior to submitting the ATO extension request;
(4) 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;
(5) Re-competing the system's contract;

(6) Completing the upgrade/replacement of major infrastructure components; or
(7) Completing the system's security assessment has been delayed due to contract issues.

m. An information system undergoing a three-year re-authorization having outstanding high or very high/critical 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 expiry to allow mitigation of the high and very high/critical vulnerabilities.

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 ispcompliance@gsa.gov.

3 Security Authorization Process

In addition to the GSA Standard A&A Process, GSA has implemented several other A&A processes for the purpose of ensuring risks to GSA IT resources are reduced to the extent possible based on budget constraints, business requirements and other resource issues. These processes and the criteria required for each are outlined below. The specific details describing each of the processes may be found in the document listed in "Document Reference" in Section 3.2 for each assessment type. Regardless of which A&A process is followed, before assessment activities for information systems begin, the following requirements must be met:

(1) The SSP is approved.
(2) The information system's architecture is approved by the OCISO Security Engineering Division (ISE).
(3) The SAP is approved.

To assist ISSOs and/ISSMs in managing recurring tasks regarding the A&A process and the security of GSA information systems an ISSO checklist was developed. A revised version of this checklist is being developed in GSA's implementation of Archer GRC, they will be used to manage these recurring tasks. In addition, a vendor ISSO checklist and companion procedural guide, CIO-IT Security-19-101, "*External System Monitoring*" identify recurring tasks that need to be completed for external vendor systems. The external vendor ISSO checklist is also being implemented in Archer GRC.

3.1 Identifying the Appropriate A&A Process/Program

Table 3-1 identifies the criteria to qualify for each A&A process.

Table 3-1. A&A Process Requirements

A&A Process/Program	Qualifying Criteria
Standard GSA Process	• All new and existing GSA information systems that do not fall under one of the other A&A processes
Lightweight Security Authorization Process	• New GSA information systems pursuing an agile development methodology • Reside on infrastructures that have a GSA ATO concurred to by the CISO or a Federal Risk and Authorization Management Program (FedRAMP) ATO • Must be FIPS 199 Low or Moderate
GSA Salesforce Process	• Applicable to applications that integrate into the main Salesforce.com application and are hosted on Salesforce.com's infrastructure • Applications developed for internal and external GSA use published on the Salesforce Platform
Security Reviews for Low Impact Software as a Service Solutions Process (LiSaaS)	• Private sector cloud computing Software as a Service (SaaS) solutions that are implemented within GSA • Duration is limited • Data already exists in the public domain or data is non-sensitive and is considered FIPS 199 Low impact • GSA would be caused limited harm regardless of the consequence of an attack or compromise • Dollar cost for such deployments do not exceed $100,000 annually
GSA Agency FedRAMP Process	• A Cloud Service Provider (CSP) requesting GSA Agency sponsorship into FedRAMP • GSA accepts sponsoring the CSP • GSA determines CSP's security authorization package will be considered FedRAMP compliant
Moderate Impact Software as a Service (MiSaaS) Security Authorization Process	• New GSA information systems pursuing an agile development methodology • Reside on infrastructures that have, or are pursuing, a Federal Risk and Authorization Management Program (FedRAMP) provisional ATO • Must be FIPS 199 Moderate
GSA Subsystem Process	• Classified as a subsystem (and not a Salesforce application) • Majority of IT security controls provided by the hosting system in which it operates • FIPS 199 Low or Moderate • FIPS 199 level can be below the level of the hosting system
GSA Information System Continuous Monitoring Program	• Must have received an initial ATO based on assessing all of the NIST SP 800-53 controls based on its FIPS 199 security categorization level and have a complete ATO package. • The information system must adhere to GSA's continuous monitoring processes and procedures as described in CIO-IT Security-12-66, including: – Deploying GSA's CDM and other enterprise ISCM tools and verifying they are operating on the platforms listed in the GSA ISCM Enterprise Management Tools Google Sheet. – Maintaining the ISCM manual processes described in Appendix A of CIO-IT Security-12-66. – Updating the system's documentation as described in Appendix A of CIO-IT Security-12-66.

3.2 A&A Process Descriptions

Additional details about the GSA A&A processes listed in Table 3-1 are provided in the following sections:

3.2.1 GSA Standard A&A Process

- **Document Reference**: Throughout this guide, process steps are described in Section 2.
- **Result**: Full 3 Year ATO
- **Summary of Process**: All new and existing GSA information systems must undergo a security assessment and authorization 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.
- **A&A Package Review & Approval Process**: Follows the process described in Section 2.5.

3.2.2 Lightweight Security Authorization Process

- **Document Reference:** IT Security Procedural Guide: Lightweight Security Authorization Process (CIO-IT Security-14-68)
- **Result:** Limited ATO (LATO) - 90 day (Sprint or Standard)/1 Year (Moderate); Full 3 Year ATO (Low)
- **Summary of Process:** New GSA information systems pursuing an agile development methodology AND residing on infrastructures that have a GSA ATO concurred by the GSA CISO or a FedRAMP ATO. 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). The following documents are required to issue a 90-day LATO:

  - Assessment Test Report (i.e., Enhanced Scanning and Assessment, Penetration)
  - POA&M
  - Certification Letter
  - ATO Letter

  A one year LATO (for FIPS 199 Moderate) or a three-year full ATO (for FIPS 199 Low) can be issued based on completing RMF Steps 1-5 as described in CIO-IT Security-14-68. The following documents are required:

  - System Security Plan (with appendices/attachments)
  - Security Assessment Report (with appendices/attachments)
  - POA&M
  - Customer Responsibility Matrix (CRM)
  - Certification Letter
  - ATO Letter

- **A&A Package Review & Approval Process**: Follows the process described in Section 2.5.

3.2.3 GSA Salesforce Platform Process

- **Document Reference:** IT Security Procedural Guide: GSA's Security Implementation of the Salesforce Platform (CIO-IT Security-11-62)
- **Result:** Salesforce Application ATO
- **Summary of Process**: Specific to applications developed for internal and external GSA use published on the Salesforce Platform. The first step is to determine the type of application. If the application is a major application, then a full Assessment and Authorization is required. If the application is a subsystem, there are key activities that should be completed. Applications are assessed and authorized in accordance with this guide, Salesforce Organization Baseline Security Configuration Settings, and specific requirements detailed in CIO-IT Security-11-62.
- **A&A Package Review & Approval Process**: After the ISSM accepts/approves the A&A package it is forwarded to the CISO for signature (i.e., no OCISO Director review).

3.2.4 Security Reviews for Low Impact Software as a Service Process

- **Document Reference:** IT Security Procedural Guide: Security Reviews for Low Impact Software as a Service (SaaS) Solutions (CIO-IT Security-16-75)
- **Result:** 1 year ATO or term of license, whichever is shorter
- **Summary of Process:** Private sector cloud computing Software as a Service (SaaS) solutions that are implemented within GSA for (1) limited duration; (2) involve data already in the public domain or data that is non-sensitive and could be considered FIPS 199 low impact, (3) GSA would be caused limited harm regardless of the consequence of an attack or compromise; and, (4) the dollar cost for such deployments do not exceed $100,000 annually. AOs must consider Federal and agency information security requirements, and the S/SO security needs. An evaluation of the data and project scope must be performed to assure the conditions noted above are met. A review of the security controls and activities for such systems must be performed to assure the security controls and practices of the contractor are adequate before authorizing use and accepting residual risk. The ATO shall only be valid for the period of the time the application license is valid or one (1) year, whichever is shorter.
- **A&A Package Review & Approval Process**: Follows the same process described in Section 2.5.

3.2.5 FedRAMP Process

- **Document Reference:** CSP Authorization Playbook-Getting Started with FedRAMP, additional details available in the FedRAMP Security Assessment Framework and FedRAMP General Document Acceptance Criteria
- **Result:** FedRAMP ATO (Agency)

- **Summary of Process:** A Cloud Service Provider (CSP) may elect to request an Agency FedRAMP 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. GSA has defined assignments for NIST SP 800-53 control parameters within the FedRAMP Low and Moderate baselines as its organizationally defined parameters. The parameters are contained in GSA's Control Tailoring Workbook. Additional information about FedRAMP is available in the reference documents and at https://www.fedramp.gov/. The CSP must provide a 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 leveraging the FedRAMP security authorization process (to attain a Government wide authorization) should contact the OCISO at ispcompliance@gsa.gov.

- **A&A Package Review & Approval Process**: Follows the FedRAMP process.

3.2.6 GSA Moderate Impact Software as a Service (MiSaaS) Security Authorization Process

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

- describes the process and requirements for authorizing the operation of Moderate Impact SaaS solutions within GSA.

- **Result:** 1 Year ATO

- **Summary of Process:** New GSA information systems pursuing an agile development methodology AND residing on infrastructures that have, or are pursuing, a FedRAMP provisional 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.

  The following documents are required as part of the ATO Package:

  - MiSaaS SSP
  - SAR, including
    - MiSaaS Test Workbook
    - OS (including DB), Web App scan data (as appropriate)
    - Penetration Test Report
  - POA&M
  - CRM
  - Certification Letter
  - ATO Letter

- **Result:** 1 Year ATO

- **Package Review & Approval Process:** Follows the process described in Section 2.5.

3.2.7 GSA Subsystem Process (previously Minor Application Process)

- **A&A Process Reference:** Described within this section.
- **Result:** ATO aligned with subsystem's hosting/supporting system.
- **Summary of Process:** This process is specific to subsystems (other than Salesforce applications) categorized with a FIPS 199 security impact level of Low or Moderate , dependent upon the resources provided by its underlying hosting/supporting system, with the underlying system providing the majority of the subsystem's security controls. The hosting/supporting 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 hosting/supporting system.

  Subsystems with a FIPS 199 security impact level of Low will adhere to and implement the controls per CIO-IT Security-14-68.

  Subsystems with a FIPS 199 security impact level of Moderate will document in a subsystem SSP all controls identified as hybrid or system specific by the underlying hosting/supporting system. These controls will be assessed using GSA's NIST 800-53 Test Cases and the results shared with the hosting/supporting system's System Owner/ISSO. All subsystems will be identified in an Appendix of their hosting/supporting system's SSP which will also be attached to the hosting/supporting system's ATO Letter. All subsystems inherit its hosting/supporting system's ATO cycle.

- **A&A Package Review & Approval Process**: Subsystems are included in the A&A Package Review & Approval Process of their hosting/supporting system. No separate ATO is issued for subsystems.

Note: When subsystems are added to a hosting/supporting system an updated listing of hosted subsystems, Appendix C of the SSP, must be maintained so the subsystem inventory is always up to date. Submit updated subsystem listings to ISP at ispcompliance@gsa.gov.

3.2.8 GSA Information System Continuous Monitoring Program

- **A&A Process Reference:** IT Security Procedural Guide: Information Security Continuous Monitoring Strategy CIO-IT Security-12-66
- **Result:** Ongoing Authorization based on continuous monitoring
- **Summary of Process:** GSA has implemented its ISCM program is summarized below.
  - Systems must meet a set of prerequisites (see Section 3.1) in order to request ongoing authorization.
  - Systems must have GSA's CDM and other enterprise ISCM tools deployed on the assets within the system boundary and verify they are operating. Tools are identified in the GSA Enterprise Continuous Monitoring Tools Google Sheet.

- Systems must maintain ISCM documentation at the frequencies defined in Appendix A of CIO-IT Security 12-66.
- Systems must maintain all NIST controls in their control sets as specified in their System Security Plans (SSP), including ensuring inherited controls are accurately documented and the controls in Appendix A of CIO-IT Security-12-66, Continuous Monitoring Controls, are updated as specified.
- Systems requiring an event-driven reauthorization must update their ongoing authorization letter to reflect re-establishment of its ongoing authorization.

- **A&A Package Review & Approval Process**: Follows the same process described in Section 2.5, with the following exception, the Director of ISP replaces the Director of IST.

4 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 Security Assessment and Authorization (CA), Planning (PL), and Risk Assessment (RA) control family implementations are addressed in this guide.

Note: GSA-IT Security-18-90, the ISPP, was developed to provide stakeholders with detailed information on the NIST SP 800-53 controls GSA has considered enterprise-wide inheritable common and hybrid controls and who the responsible party is for implementing the control. In the following sections when a control implementation is covered in the ISPP the control's subsection will refer to the ISPP for parameter assignments and implementation guidance.

Table 4-1, NIST SP 800-53 Control to CSF Mapping, provides how the NIST SP 800-53 controls within this guide are aligned with the CSF Category Unique Identifier Codes. Table A-1 in Appendix A provides details on the Category and Subcategory definitions and the unique identifiers listed.

Table 4-1: NIST SP 800-53 Control to CSF Mapping

NIST SP 800-53 Control	CSF Category Unique Identifier Code
CA-1	ID.GV-1, ID.GV-3
CA-2	ID.RA-1, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.CO-3
CA-3	ID.AM-3, DE.AE-1
CA-5	Not Mapped in the CSF
CA-6	Not Mapped in the CSF
CA-7	ID.RA-1, PR.IP-7, PR.IP-8, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.CO-3, RS.AN-1, RS.MI-3
CA-8	ID.RA-1
CA-9	ID.AM-3
PL-1	ID.GV-1, ID.GV-3
PL-2	PR.IP-7, DE.DP-5
PL-4	Not Mapped in the CSF
PL-8	ID.AM-3, PR.IP-2, PR.PT-5

RA-1	ID.GV-1, ID.GV-3
RA-2	ID.AM-5, ID.RA-4, ID.RA-5, ID.SC-2
RA-3	ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.SC-2, PR.IP-12, DE.AE-4, RS.MI-3
RA-5	ID.RA-1, PR.IP-12, DE.CM-8, DE.DP-4, DE.DP-5, RS.CO-3, RS.MI-3

4.1 Security Assessment and Authorization (CA)

4.1.1 CA-1 Security Assessment and Authorization Policy and Procedures

Parameter assignments and implementation guidance for the CA-1 control are provided in CIO-IT Security-18-90.

4.1.2 CA-2 Security Assessments

Control: The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:
    1. Security controls and control enhancements under assessment;
    2. Assessment procedures to be used to determine security control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information 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 requirements;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment to [*personnel with system security responsibilities as identified in CIO 2100.1 and CIO-IT Security 06-30*].

Control Enhancements:

(1) The organization employs assessors or assessment teams with [*independence where 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*] to conduct security control assessments

(2) The organization includes as part of security control assessments, [*annual*], [*announced*], [*penetration testing*].

GSA Implementation Guidance:

GSA requires a security control assessment to be performed for all information systems as part of the security authorization/re-authorization process. The security control assessment must include GSA's NIST 800-53 Test Cases. The security control assessment must document the

implementation status in sufficient detail in order to assist in determining the overall effectiveness of all controls and enhancements that have been selected and implemented for the system as per FIPS-199 impact level.

GSA's process for performing a security control assessment is fully defined in Section 2.4 of this guide, RMF Step 4 – Assess Security Controls. The results of the security control assessment must be documented in a SAR.

As per CA-2, Enhancement (1), GSA FIPS 199 Moderate and High Impact Systems must be assessed by an independent third party. The use of an independent assessment team reduces the potential for impartiality or conflicts of interest, when verifying the implementation status and effectiveness of the security controls.

CA-2, Enhancement (2), requires GSA FIPS High Impact Systems to 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.

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the controls IAW the guidance and control parameters established above.*

4.1.3 CA-3 System Interconnections

Control: The organization:

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Reviews and updates Interconnection Security Agreements [*at least annually*].

Control Enhancements:

(5) The organization employs [*deny-all, permit-by-exception*] policy for allowing [*all GSA systems*] to connect to external information systems.

GSA Implementation Guidance:

The focus of this control is to ensure that any persistent connection to any other information system outside of the system's authorization boundary has been approved by the AO, identified and documented within the SSP, and monitored on an ongoing basis.

Chapter 3 of GSA CIO 2100.1 outlines the following interconnection requirements:

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

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 system security plan and that limits access only to the information needed by the other system; and

All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be approved by the GSA CISO.

The terms "connection" or "interconnection" in this case, means any on-going, persistent or substantial interaction with any information system(s) that is located outside of the authorization boundary. These connections can be physical and/or logical, and include data entering or exiting to/from the authorization boundary. User-controlled connections such as email, ftp, remote access, and web browsing are not considered interconnections and therefore do not apply to this control.

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the controls IAW the guidance and control parameters established above.*

4.1.4 CA-5 Plan of Action and Milestones

Control: The organization:

a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and milestones [*at least quarterly*] based on the findings from security impact analyses, and continuous monitoring activities.

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 which details the POA&M processes and procedures for meeting the requirements of this control.

On a quarterly basis, POA&Ms must be provided to the OCISO in order to monitor agency-wide remediation efforts as required by OMB policy. These updates should be performed as POA&M updates occur throughout the fiscal year using the system POA&M which is maintained by the system ISSO or ISSM and located on the system POA&M Team Drives for OCISO review. The POA&M Team Drives serve as the primary location for managing and communicating GSA's system and program POA&Ms, and is available internally at GSA, or via VPN. New systems that are currently undergoing security authorization process or that have not been included in the GSA FISMA inventory must use the POA&M Template available on GSA Guidance Team Drive or by contacting ispcompliance@gsa.gov.

Additional Contractor System Considerations:
Contractor systems must provide POA&Ms through their ISSO(s) as contractors will not have access to the POA&M Team 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). 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 Team Drives.

4.1.5 CA-6 Security Authorization

Control: The organization:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;
b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
c. Updates the security authorization [*every three (3) years or when a significant change occurs as defined in NIST SP 800-37,Revision 2, Appendix F*].

GSA Implementation Guidance:
The focus of this control is to ensure that all information systems which have been authorized to operate before being placed into operational status. All information systems must undergo authorization/reauthorization every three years or when there is a significant change as defined in NIST SP 800-37, Appendix F, following the security authorization process documented in this guide. Detailed procedures for the security authorization process can be found in Section 2.5 of this guide, RMF Step 5 – Authorize Information System. Additional ATO or authorization types exist in GSA and are described in Section 3.2 of this document.

The explicit acceptance of *risk* is the responsibility of the AO. The AO must consider many factors, balancing security considerations with mission and operational needs. The AO issues an authorization decision for the information system and the common controls inherited by the system after reviewing the security authorization package submitted by the System Owner. The security authorization package provides the AO with the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

The security authorization package includes:

- SSP (required policies and procedures (as requested by GSA), Rules of Behavior, Interconnection Agreements (as applicable), GSA 800-53 Control Tailoring Workbook, and appropriate Control Implementation Summary Table);
- Security Assessment Report (with required appendices [see Appendix C]);
- POA&M;
- Penetration Test Report, if applicable;
- Code Review Report (Strongly Recommended);
- Contingency Plan;
- Contingency Plan Test Report;
- Certification Letter
- ATO Letter.

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. Following review of the security authorization package and consultation with key agency officials, the AO must render an authorization decision to:

- Authorize system operation w/out any restrictions or limitations on it operation;
- Authorize system operation w/ restriction or limitation on its operation. The POA&M must include detailed corrective actions to correct deficiencies. Resubmit an updated security authorization package upon completion of required POA&M actions to move to ATO w/out any restrictions; or
- Not authorized for operation.

Questions concerning the security authorization process, significant changes, or CIO 2100.1 can be directed to ispcompliance@gsa.gov.

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the controls IAW the guidance and control parameters established above.*

4.1.6 CA-7 Continuous Monitoring

Parameter assignments and implementation guidance for the CA-7 control are provided in CIO-IT Security-18-90.

CIO-IT Security-12-66 provides detailed information on the implementation of GSA's Information System Continuous Monitoring Program.

4.1.7 CA-8 Penetration Testing

Control: The organization conducts 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:

(1) The organization employs 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).*

GSA Implementation Guidance:
All Internet accessible, FIPS 199 High impact, and HVA information systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of the A&A package. Annual penetration tests can be completed internally and do not require an independent assessor.

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the controls IAW the guidance and control parameters established above.*

4.1.8 CA-9 Internal System Connections

Control: The organization:

a. Authorizes internal connections of [*other GSA systems using a secure methodology providing security commensurate with the acceptable level of risk as defined in the*

system security plan and limits access to the information needed by the connected system] to the information system; and

b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

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 system security plan and that limits access only to the information needed by the other system.

4.2 Planning (PL)

4.2.1 PL-1 Security Planning Policy and Procedures

Parameter assignments and implementation guidance for the PL-1 control are provided in CIO-IT Security-18-90.

4.2.2 PL-2 System Security Plan

Control: The organization:

a. Develops a security plan for the information system that:

1. Is consistent with the organization's enterprise architecture;
2. Explicitly defines the authorization boundary for the system;
3. Describes the operational context of the information system in terms of missions and business processes;
4. Provides the security categorization of the information system including supporting rationale;
5. Describes the operational environment for the information system and relationships with or connections to other information systems;
6. Provides an overview of the security requirements for the system;
7. Identifies any relevant overlays, if applicable;
8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distributes copies of the security plan and communicates subsequent changes to the plan to [*personnel with IT security responsibilities for the system as defined in GSA CIO Order 2100.1*];

c. Reviews the security plan for the information system [*annually*];

d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

e. Protects the security plan from unauthorized disclosure and modification.

Control Enhancements:

(3) The organization plans and coordinates security-related activities affecting the information system with [*personnel with IT security responsibilities for the system as defined in GSA CIO Order 2100.1*] before conducting such activities in order to reduce the impact on other organizational entities.

GSA Implementation Guidance:

The focus of this control is to ensure that a 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 NIST SP 800-18. Detailed guidance is available in RMF Step 1 – Categorize Information System, RMF Step 3 – Implement Security Controls, and Section 3, of this guide.

The security requirements per FIPS 199 impact level and the security controls which are planned or in-place to meet these requirements, must be documented within the SSP and updated as-needed to reflect any change to the information system environment. Updates made to the SSP must include updates to system applications and hardware, remediation of previously identified weaknesses and any addition of new weaknesses identified through security assessments or continuous monitoring.

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the controls IAW the guidance and control parameters established above.*

4.2.3 PL-4 Rules of Behavior

Parameter assignments and implementation guidance for the PL-4 control are provided in CIO-IT Security-18-90.

4.2.4 PL-8 Information Security Architecture

Control: The organization:

a. Develops an information security architecture for the information system that:
    1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
    2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
    3. Describes any information security assumptions about, and dependencies on, external services;

b. Reviews and updates the information security architecture [*at least annually*] to reflect updates in the enterprise architecture; and

c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

GSA Implementation Guidance:
GSA's CIO-IT Security-19-95, "Security Engineering Architecture Reviews," requires every system seeking authorization to have their architecture approved by ISE before beginning security assessment activities. It also requires reviews of any changes/updates to the information security architecture at least annually to assess system changes and changes/updates in GSA's enterprise architecture.

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the controls IAW the guidance and control parameters established above.*

4.3 Risk Assessment (RA)

4.3.1 RA-1 Risk Assessment Policy and Procedures

Parameter assignments and implementation guidance for the RA-1 control are provided in CIO-IT Security-18-90.

4.3.2 RA-2 Security Categorization

Control: The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

GSA Implementation Guidance:
GSA system owners, data owners, ISSOs, and ISSMs are required to follow the processes and procedures described in Section 2.1 of this guide for determining the security categorization of their information and information systems.

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the controls IAW the guidance and control parameters established above.*

4.3.3 RA-3 Risk Assessment

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in [*Security Assessment Report (SAR*)];

c. Reviews risk assessment results [*every three (3) years or with a significant change as defined in NIST SP 800-37 Revision 2, Appendix F*]; and
d. Disseminates risk assessment results to [*personnel with risk assessment/management responsibilities as defined in GSA CIO Order 2100.1*]; and
e. Updates the risk assessment [*every three (3) years or with a significant change as defined in NIST SP 800-37 Revision 2, Appendix F*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

GSA Implementation Guidance:
The focus of this control is to verify that an assessment of risk is performed and documented for the information system and that the subsequent security assessment report is communicated to GSA senior management, in order to provide key information regarding the system's current security state and resulting risk to GSA operations, assets, and individuals. The results of the risk assessment provide critical information to assist the GSA AO in determining whether or not to authorize/re-authorize the information system.

GSA requires a risk assessment to be conducted as part of a system's initial security authorization process, and then risk is assessed in accordance with the specific GSA A&A process used from Section 3. GSA's process for performing a risk assessment is defined in Section 2.4 of this guide and in the GSA A&A process guides listed in Appendix B. The results of this risk assessment must be documented as defined in the GSA A&A process used.

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the controls IAW the guidance and control parameters established above.*

4.3.4 RA-5 Vulnerability Scanning

Parameter assignments and implementation guidance for the RA-5 control are provided in CIO-IT Security-18-90.

5 Additional NIST Controls Required by GSA

GSA requires certain controls be a part of a systems control set, regardless of a system's specific A&A process, in accordance with the applicability listed in the following table.

Table 5-1: GSA Additional NIST Control Requirements

Control No.	Control Name/Statement	Control Applicability
CA-8	**Penetration Testing** The organization conducts penetration testing [*during A&A efforts and annually thereafter]* on *[all Internet accessible, FIPS 199 High impact, and High Value Asset (HVA) information systems*].	• All Internet accessible, FIPS 199 High, and HVA information systems

Control No.	Control Name/Statement	Control Applicability
CA-8(1)	**Penetration Testing | Independent Penetration Agent or Team.** The organization employs 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)	• All Internet accessible, FIPS 199 High, and HVA information systems
CM-2(2)	**Baseline Configuration | Automation Support for Accuracy / Currency** The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	• Standard A&A Moderate and High Systems • Lightweight A&A Systems • MiSaaS A&A Systems • ISCM Program
CM-6(1)	**Configuration Settings | Automated Central Management / Application / Verification** The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*all operating systems*].	• Standard A&A Moderate and High Systems • Lightweight A&A Systems • MiSaaS A&A Systems • ISCM Program
CM-8(2)	**Information System Component Inventory | Automated Maintenance** The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	• Standard A&A Moderate and High Systems • Lightweight A&A Systems • ISCM Program
CM-8(6)	**Information System Component Inventory | Assessed Configurations / Approved Deviations** The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.	• Standard A&A Moderate and High Systems
PL-8	**Control: The organization:** a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture [*at least annually*] to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.	• All Systems
SA-8	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	• All Systems

Control No.	Control Name/Statement	Control Applicability
SA-22	**Unsupported System Components** The organization: a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	• All Systems
SC-28(1)	**Protection of Information at Rest | Cryptographic Protection** The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [(1) Personally identifiable information; (2) Payment Card Industry data; (3) Authenticators, including but not limited to passwords, keys, and tokens; (4) business sensitive data as determined by the data owner and approved by the AO] on [any system component, including databases (i.e., table, column, or filed level) and applications].	• All Systems
SI-2(3)	**Flaw Remediation | Time to Remediate Flaws / Benchmarks for Corrective Actions** The organization: a. Measures the time between flaw identification and flaw remediation; and b. Establishes [(1) For Internet-accessible IP addresses (a) Any Critical (Very High) scan vulnerabilities must be remediated within 15 days. (b) Any High scan vulnerabilities must be remediated within 30 days. (c) Any Moderate scan vulnerabilities must be remediated within 90 days. (2) For all other assets (a) Any Critical (Very High) and High scan vulnerabilities must be remediated within 30 days. (b) Any Moderate scan vulnerabilities must be remediated within 90 days.] for taking corrective actions.	• Standard A&A Moderate and High Systems • ISCM Program
SI-3(7)	**Malicious Code Protection | Nonsignature-Based Detection** The information system implements nonsignature-based malicious code detection mechanisms.	• Standard A&A Moderate and High Systems • MiSaaS A&A Systems

6 Summary

Managing enterprise-level risk through a system life cycle perspective is a departure from the traditional view of security authorization as a static, procedural process. GSA has integrated EO 13800 and the NIST CSF throughout this guide by showing how they align with GSA's agency-wide use of the NIST RMF security authorization processes. The policies and procedures outlined in this guide provide an effective approach to system security authorization that is more dynamic and more capable of managing information system-related security risks across a diverse enterprise.

All GSA information systems must undergo a security control assessment and be authorized to operate according to their specific A&A process. GSA's standard A&A process requires A&A at least every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST SP 800-37.

GSA contractors and Federal employees should use this guide and the noted references prior to selecting and performing a security authorization process. Where there is a conflict between NIST guidance and GSA guidance, contact OCISO at ispcompliance@gsa.gov.

Note: In Appendix F, Table F-1, GSA has identified a list of NIST SP 800-53 controls considered to be Showstopper Controls. Showstopper controls, if not fully compliant, will keep a system from receiving a full ATO.

Appendix A: CSF Function, Category, and Subcategory Definitions/NIST SP 800-53 Control Mapping

The five CSF core function definitions are:

- **Identify (ID):** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.
- **Protect: (PR):** Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
- **Detect (DE):** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- **Respond (RS):** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.
- **Recover (RC):** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

Table A-1, CSF Category/Subcategory to NIST SP 800-53 Controls, provides a mapping between the CSF Subcategory Unique Identifiers and descriptions and NIST SP 800-53 controls. GSA is aligned with the CSF via the use of the NIST SP 800-53 controls shown in Table A-1. Additional information is available about the CSF in NIST CSF Version 1.1.

Table A-1: CSF Category/Subcategory to NIST SP 800-53 Controls

Category/Subcategory	NIST SP 800-53 Controls
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities 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-1: Physical devices and systems within the organization are inventoried	CM-8, PM-5
ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8, PM-5
ID.AM-3: Organizational communication and data flows are mapped	AC-4, CA-3, CA-9, PL-8
ID.AM-4: External information systems are catalogued	AC-20, SA-9
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14, SC-6
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CP-2, PS-7, PM-11
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	
ID.BE-1: The organization's role in the supply chain is identified and communicated	CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	CP-2, CP-11, SA-13, SA-14
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	
ID.GV-1: Organizational cybersecurity policy is established and communicated	-1 controls from all families
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	PM-1, PM-2, PS-7
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	-1 controls from all families
ID.GV-4: Governance and risk management processes address cybersecurity risks	SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
ID.RA-1: Asset vulnerabilities are identified and documented	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	PM-15, PM-16, SI-5
ID.RA-3: Threats, both internal and external, are identified and documented	RA-3, SI-5, PM-12, PM-16
ID.RA-4: Potential business impacts and likelihoods are identified	RA-2, RA-3, PM-9, PM-11, SA-14

Category/Subcategory	NIST SP 800-53 Controls
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	RA-2, RA-3, PM-16
ID.RA-6: Risk responses are identified and prioritized	PM-4, PM-9
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	PM-9
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	PM-9
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	PM-8, PM-9, PM-11, SA-14
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	SA-9, SA-12, PM-9
ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan	SA-9, SA-11, SA-12, PM-9
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations	AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
PR.AC-3: Remote access is managed	AC-1, AC-17, AC-19, AC-20, SC-15
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
PR.AC-5: PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	AC-4, AC-10, SC-7
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	
PR.AT-1: All users are informed and trained	AT-2, PM-13
PR.AT-2: Privileged users understand roles and responsibilities	AT-3, PM-13

Category/Subcategory	NIST SP 800-53 Controls
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	PS-7, SA-9, SA-16
PR.AT-4: Senior executives understand roles and responsibilities	AT-3, PM-13
PR.AT-5: Physical and information security personnel understand roles and responsibilities	AT-3, IR-2, PM-13
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	
PR.DS-1: Data-at-rest is protected	MP-8, SC-12, SC-28
PR.DS-2: Data-in-transit is protected	SC-8, SC-11, SC-12
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	CM-8, MP-6, PE-16
PR.DS-4: Adequate capacity to ensure availability is maintained	AU-4, CP-2, SC-5
PR.DS-5: Protections against data leaks are implemented	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SC-16, SI-7
PR.DS-7: The development and testing environment(s) are separate from the production environment	CM-2
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	SA-10, SI-7
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
PR.IP-2: A System Development Life Cycle to manage systems is implemented	PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
PR.IP-3: Configuration change control processes are in place	CM-3, CM-4, SA-10
PR.IP-4: Backups of information are conducted, maintained, and tested	CP-4, CP-6, CP-9
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
PR.IP-6: Data is destroyed according to policy	MP-6
PR.IP-7: Protection processes are improved	CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
PR.IP-8: Effectiveness of protection technologies is shared	AC-21, CA-7, SI-4
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
PR.IP-10: Response and recovery plans are tested	CP-4, IR-3, PM-14
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
PR.IP-12: A vulnerability management plan is developed and implemented	RA-3, RA-5, SI-2
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	MA-2, MA-3, MA-5, MA-6
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	MA-4
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	

Category/Subcategory	NIST SP 800-53 Controls
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU Family
PR.PT-2: Removable media is protected and its use restricted according to policy	MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	AC-3, CM-7
PR.PT-4: Communications and control networks are protected	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4
DE.AE-2: Detected events are analyzed to understand attack targets and methods	AU-6, CA-7, IR-4, SI-4
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
DE.AE-4: Impact of events is determined	CP-2, IR-4, RA-3, SI-4
DE.AE-5: Incident alert thresholds are established	IR-4, IR-5, IR-8
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	
DE.CM-1: The network is monitored to detect potential cybersecurity events	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	CA-7, PE-3, PE-6, PE-20
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
DE.CM-4: Malicious code is detected	SI-3, SI-8
DE.CM-5: Unauthorized mobile code is detected	SC-18, SI-4, SC-44
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
DE.CM-8: Vulnerability scans are performed	RA-5
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	CA-2, CA-7, PM-14
DE.DP-2: Detection activities comply with all applicable requirements	AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
DE.DP-3: Detection processes are tested	CA-2, CA-7, PE-3, PM-14, SI-3, SI-4, PM-14
DE.DP-4: Event detection information is communicated	AU-6, CA-2, CA-7, RA-5, SI-4
DE.DP-5: Detection processes are continuously improved	CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Category/Subcategory	NIST SP 800-53 Controls
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity events.	
RS.RP-1: Response plan is executed during or after an incident	CP-2, CP-10, IR-4, IR-8
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	
RS.CO-1: Personnel know their roles and order of operations when a response is needed	CP-2, CP-3, IR-3, IR-8
RS.CO-2: Incidents are reported consistent with established criteria	AU-6, IR-6, IR-8
RS.CO-3: Information is shared consistent with response plans	CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	CP-2, IR-4, IR-8
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	PM-15, SI-5
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	
RS.AN-1: Notifications from detection systems are investigated	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
RS.AN-2: The impact of the incident is understood	CP-2, IR-4
RS.AN-3: Forensics are performed	AU-7, IR-4
RS.AN-4: Incidents are categorized consistent with response plans	CP-2, IR-4, IR-5, IR-8
RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	SI-5, PM-15
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	
RS.MI-1: Incidents are contained	IR-4
RS.MI-2: Incidents are mitigated	IR-4
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	CA-7, RA-3, RA-5
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
RS.IM-1: Response plans incorporate lessons learned	CP-2, IR-4, IR-8
RS.IM-2: Response strategies are updated	CP-2, IR-4, IR-8
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	
RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	CP-10, IR-4, IR-8
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	
RC.IM-1: Recovery plans incorporate lessons learned	CP-2, IR-4, IR-8
RC.IM-2: Recovery strategies are updated	CP-2, IR-4, IR-8
Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	
RC.CO-1: Public relations are managed	N/A
RC.CO-2: Reputation after an event is repaired	N/A
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	CP-2, IR-4

Appendix B: Consolidated List of Guidance, Policies, Procedures, Templates

Federal Regulations/Guidance:

- DHS Cybersecurity Directives
- EO 13800, *"Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"*
- FIPS 199, *"Standards for Security Categorization of Federal Information and Information Systems"*
- NIST CSF, *"Framework for Improving Critical Infrastructure Cybersecurity"*
- 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, *"Security Guide for Interconnecting Information Technology Systems"*
- NIST SP 800-53, Revision 4, *"Security and Privacy Controls for Federal Information Systems and Organizations"*
- NIST SP 800-60, Volume I, Revision 1, *"Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories"*
- NIST SP 800-60, Volume II, Revision 1, *"Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories"*
- NIST SP 800-64, Revision 2, *"Security Considerations in the Information System Development Life Cycle"*
- Public Law 113-283, "*Federal Information Security Modernization Act of 2014*"

GSA Guidance:

- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2140.4, "*Information Technology (IT) Solutions Life Cycle (SLC) Policy*"

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

- GSA CIO-IT Security-01-05, *"Configuration Management"*
- GSA CIO-IT Security-06-30, "*Managing Enterprise Risk*"
- GSA CIO-IT Security-06-32, "*Media Protection*"
- GSA CIO-IT Security-07-35, "*Web Application Security*"
- GSA CIO-IT Security-09-44, "*Plan of Action and Milestones*"
- GSA CIO-IT Security-09-48, "*Security Language for IT Acquisition Efforts*"
- GSA CIO-IT Security-11-51, "*Conducting Penetration Test Exercises*"
- GSA CIO-IT Security-11-62, "*GSA's Security Implementation of the Salesforce Platform*"
- GSA CIO-IT Security-12-66, "*Information Security Continuous Monitoring Strategy*"
- GSA CIO-IT Security-14-68, "*Lightweight Security Authorization Process*"

- GSA CIO-IT Security-16-75, "*Security Review for Low Impact Software as a Service (SaaS) Solutions*"
- GSA CIO-IT Security-18-88, "*Moderate Impact Software as a Service (MiSaaS) Security Authorization Process"*
- GSA CIO-IT Security-18-90, "*Information Security Plan"*
- GSA CIO-IT Security-18-91, "*Risk Management Strategy"*
- GSA CIO-IT Security-19-95, *"Security Engineering Architecture Reviews"*
- GSA CIO-IT Security-19-101, "*External Information System Monitoring*"

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

- FIPS 199 Security Categorization Template
- Digital Identity Acceptance Statement
- GSA Control Tailoring Workbook
- Low, Moderate, and Control Summary Tables
- Low, Moderate, and High System Security Plan Templates
- Low, Moderate, and High NIST 800-53 Rev 4 Test Cases
- Security Assessment Plan Template
- Security Assessment Report Template
- ATO Letter Template
- Certification Letter Template
- Low, Moderate, and High Contingency Plan Templates
- Contingency Plan Test Report
- Interconnection Security Agreement Template
- MiSaaS Test Workbook
- MiSaaS SSP Template
- Penetration Test Exercise Templates:
  - Kickoff Meeting Presentation Template
  - Penetration Test Rules of Engagement Template
  - Authorization Memorandum Template
  - Test Findings Template
  - Penetration Test Report Template
- POA&M Team Drive User Access Request (if access to a POA&M Team Drive is not already provided)
- ISCM Plan Template
- ISCM Ongoing Authorization Letter Template
- Salesforce Platform Documentation
- Transfer and Disposal Notification Templates

Privacy Threshold Analysis/Privacy Impact Assessment forms, templates and information are available on GSA's IT Privacy page.

Appendix C: 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 IT Security Forms page, procedural guides are available on the IT Security Procedural Guides page. Search for the title of the template/form/document listed to obtain its current version. Additional documents may be required of contractor systems as identified in CIO-IT Security-19-101.

Standard A&A Process
Documents
System Security Plan (Low, Moderate, High) Appendix A - Acronyms, Terms, and Definitions Appendix B - References Appendix C - Hosted Subsystems (if applicable) Other Appendices, as necessary Attachment 1: Privacy Threshold Analysis / Privacy Impact Assessment Attachment 2: FIPS 199 Security Categorization Attachment 3: Digital Identity Acceptance Statement Attachment 4: Interconnection Security Agreement Attachment 5: Control Summary Table (Low, Moderate, High) Attachment 6: Contingency Plan (Low, Moderate, High) Attachment 7: Contingency Plan Test Report Attachment 8: Incident Response Plan Attachment 9: Incident Response Plan Test Report Attachment 10: Configuration Management Plan Attachment 11: Continuous Monitoring Plan (if applicable) Attachment 12: Code Review Report (if applicable) Other Attachments, as necessary
Security Assessment Report (Results from the Security Assessment Plan) Appendix A - Acronyms, Terms, and Definitions Appendix B - NIST 800-53 Test Cases Appendix C - Operating System Scanning Results Appendix D - Database Application Scanning Results Appendix E - Web Application Scanning Results Other Appendices, as necessary Attachment 1: Penetration Test Report Other Attachments, as necessary
Plan of Action and Milestones (POA&M)
Certification Letter
ATO Letter

Lightweight Security Authorization Process
Documents
System Security Plan (with appendices/attachments) Security Assessment Report (with appendices/attachments)
POA&M
CRM - Please contact your Information System Security Manager (ISSM) to receive the vendor's current CRM for your system.
Certification Letter
ATO Letter

GSA Salesforce Process
Documents
GSA CIO-IT Security-11-62, "*GSA's Security Implementation of the Salesforce Platform*," contains specific instructions concerning the Salesforce-specific templates identified below (identified by an asterisk) and where a URL is not available.
*Implementation of Subsystems * a. COE Security Process 2016 * b. App Config Example * c. Security Controls Analysis Template * d. Salesforce App Review Process Template
*Salesforce Guide 11-62 Section 4_8 Controls
*Salesforce Security Plan Customer Controls - This document is controlled and is available by contacting the Salesforce ISSM or ISSO.
*Example Salesforce Organization Baseline
*SF Security Settings
*Salesforce Security Implementation Guide - Spring 2016
*A Guide to Sharing Architecture
*SF Security Configuration Options
*User Request Form Salesforce Template
*External Access to GSA Salesforce User
Privacy Threshold Analysis / Privacy Impact Assessment
Code Scan Reviews
Plan of Action and Milestones (POA&M)
Certification Letter
ATO Letter

Security Reviews for Low Impact Software as a Service Solutions Process
Documents
Documented results of required review activities, including:
Assign a unique ID to each person. Users must be individually identified (Reference NIST SP 800-53 control IA2 - Identification and Authentication). When possible, Two Factor Authentication (2FA) should be used for user logons.
Document and implement system and security parameters deferred to customers. Do not use the vendor-supplied defaults for system passwords and other security parameters. GSA security policies and best practices should be used to the greatest extent possible.
All transmissions of authentication credentials must be encrypted (e.g., TLS over HTTPS). It is strongly recommended that the entire session be encrypted.
Perform web application scanning (e.g., WebInspect, Acunetix, Burp Suite Pro, etc.) annually. The OCISO can assist with web application scans if vendor(s) do not have an in house web application scanning capability.
Perform operating system (OS) vulnerability scanning (e.g., Nessus, Qualys, nCircle, McAfee Vulnerability Manager, etc.). a. Vendors that are Payment Card Industry Data Security Standard (PCI DSS) compliant or have the McAfee Secure Seal or TrustGuard Quarterly Scanned Seal must provide the results of their latest PCI DSS Compliant, McAfee Secure Seal or TrustGuard quarterly scan. b. Vendors that do not meet the PCI DSS, McAfee, or TrustGuard standards listed, must provide their most recent OS vulnerability scan results.
Verify that the vendor has an acceptable flaw remediation process exists. Vendors must be able to identify and remediate information system flaws in a timely manner (i.e., how often scans are completed and how vulnerabilities are remediated). Reference NIST 800-53 control SI2 – Flaw Remediation.
Vendor shall either provide the results of their Service Organization Control (SOC) 2/Statements on Standards for Attestation Engagements (SSAE) 16 audit report and/or have one of the following vendor certifications SysTrust, WebTrust (American Institute of Certified Public Accountants (AICPA)-sponsored), ISO/IEC 27001, or PCI DSS Compliance. The SSAE/SOC 2 is not a form of security certification but it does provide independent third party attestation of the provider's general operating environment and supporting processes. Vendors may also provide evidence of PCI security assessments, self-testing, and records from other external audits and assessors to supplement the SSAE/SOC 2 audit report or vendor certifications. Vendors are strongly encouraged to present as much information as possible to allow an adequate understanding of the applications security posture and a determination of risk. Although the minimum requirement is for the SSAE/SOC 2 audit report or one of the vendor certifications; the GSA AO and the CISO will take a holistic view of the application based on all of the documentation presented to determine the overall risk of the application as well as any residual risks that may need to be accepted when considering the application for use. If the documentation presented does not provide an adequate understanding of the systems security posture and/or is deemed insufficient to make a risk determination; additional information will be required.
Certification Letter
ATO Letter

GSA Agency FedRAMP Process
Documents
Note: The FedRAMP A&A documentation templates are available on the FedRAMP website under Documents and Templates. Please visit that website to get the current templates.
System Security Plan
Security Assessment Plan
NIST 800-53 Revision 4 Test Cases
Security Assessment Report
(Vendors) Users Guide)
Control Implementation Summary
POA&M
FIPS 199 Categorization
e-Authentication Level
Rules of Behavior
(Vendors) Configuration Management Plan
(Vendors) Information System Security Policies
IT Contingency Plan
(Vendors) Incident Response Plan
Privacy Threshold Analysis and PIA

Moderate Impact Software as a Service (MiSaaS) Security Authorization Process
Documents
System Security Plan MiSaaS SSP Template
Security Assessment Report Security Assessment Report (including, as applicable) • MiSaaS Test Workbook • Vulnerability Scan Data • Penetration Test Report
POA&M
CRM - Please contact your Information System Security Manager (ISSM) to receive the vendor's current CRM for your system.
Certification Letter
ATO Letter

GSA Subsystem A&A Process
Documents
FIPS 199 Low Subsystem
See Lightweight Security Authorization Process Documentation)
FIPS 199 Moderate Subsystem
System Security Plan (Low, Moderate, High) (only hybrid and system specific controls)
NIST 800-53 Test Cases (only hybrid and system specific controls)
Security Assessment Report (only hybrid and system specific controls)

GSA Information System Continuous Monitoring Program
Documents
ISCM ATO Package • ISCM Plan, including (as attachments): – System Security Plan – POA&M – FISMA Self-Assessment Results – OS Vulnerability scan results – Unauthenticated Web Vulnerability scan results (as applicable) – Authenticated Web Vulnerability scan results (as applicable) – Penetration Test Results (as applicable) – Hardware Asset Inventory Report generated by automated tool – Software Asset Inventory Report generated by automated tool – Configuration Compliance scan results – Configuration Management Plan – IT Contingency Plan – IT Contingency Plan Test Results – Incident Response Plan – Incident Response Plan Test Results – Privacy Threshold Analysis and Privacy Impact Assessment (PIA) (as applicable)
ISCM Ongoing Authorization Letter

Appendix D: GSA Defined Cloud Controls

GSA's Control Tailoring Workbook contains a Sheet (Tab) with GSA's assignment parameters for GSA Cloud Control Settings for FIPS 199 Low and Moderate baselines. These parameter settings must be used by CSPs working with GSA pursuing an authorization under the FedRAMP program. CSPs must also address the other controls in FedRAMP's baselines using FedRAMP's assignment parameters.

Appendix E: Scanning Frequency By A&A Process

Scanning/testing frequency by component type and A&A process are listed in the 06-30 Scanning Parameter Spreadsheet.

Appendix F: Showstopper Controls

Table F-1 lists the NIST SP 800-53 controls that GSA has identified as Showstopper Controls. Showstopper controls, if not fully compliant, will keep a system from receiving a full ATO.

Table F-1: GSA Showstopper Controls

#	Showstopper Description	Control Reference
1	Multi-Factor Authentication (MFA) for Privileged & User-level access: FIPS 199 Low, Moderate and High systems shall utilize a GSA-approved multi-factor authentication mechanism for privileged authentication. FIPS 199 Moderate and High shall utilize a GSA-approved multi-factor authentication mechanism for non-privileged authentication (Note: Future NIST guidance will include/require IA-2(2) for FIPS 199 Low systems). All systems which require authentication, regardless of FIPS 199-impact level shall implement multi-factor authentication for user-level authentication. Further, systems leveraging certificate-based authentication shall not be downgraded to only user name and password authentication. Per NIST 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management, 2FA methods involving the sending of PINS/passwords via email is prohibited and on public networks via SMS is restricted. Sending PINS/passwords to registered telephone numbers to GFE is allowed based on a risk analysis. 2FA methods shall favor approaches that do not expose PINS/passwords to intercept risk including but not limited to HOTP, TOTP, SAML/OIDC, PIV, FIDO/WebAuthn. 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-2 (1) Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts IA-2 (2) Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts
2	Critical and High vulnerabilities: IT Security Procedurals Guide: Managing Enterprise Risk [CIO IT Security 06-30] identifies 'Ongoing Remediation Actions' requirements. If an assessment identifies 'Ongoing Remediation Actions' are not being addressed, per the stated policy, then the system will not be approved for a 3 year ATO or OA, until the risk is mitigated.	SI-2 Flaw Remediation
3	Remote Code Execution (RCE) Vulnerabilities: Remote Code Evaluation (RCE) is a vulnerability that can be exploited if user input is injected into a File or a String and executed (evaluated) by the programming language's parser. Regardless of the RCE system impact level identified. 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-2 Flaw Remediation

#	Showstopper Description	Control Reference
4	EOL Software: 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 Acceptance of Risk (AOR), are the possible documentation outcome requirements of the risk evaluation. 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.	SA-22 Unsupported System Components
5	System Architecture has been reviewed and approved by ISE: IT Security Procedurals Guide: IT Security Procedurals Guide: Security Engineering Architecture Reviews [CIO IT Security 19-95] identifies the OCISO Security Engineering (ISE) system evaluation requirements. If an assessment identifies an ISE system review has not been completed for the system. The system will not be approved for a 3 year ATO or OA, until one is completed.	PL-8 Information Security Architecture SA-8 Security Engineering Principles
6	Integration with GSA's Security Stack (Internal Systems): System integration includes; • Enterprise Logging Platform (ELP) (AU-6(1)) • BigFix (CM-6) • Bit9 (CM-7) • Tenable Security Center (TSC) & NetSparker Monthly Non-Auth Web Scans (RA-5) • Cylance AV & (SI-3) • FireEye (SI-4) • OSEC (SI-7) If an assessment identifies the system has not been integrated with the 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.	AU-6(1) Audit Review, Analysis, and Reporting CM-6 Configuration Settings CM-7 Least Functionality RA-5 Vulnerability Scanning SI-3 Malicious Code Protection SI-4 Information System Monitoring SI-7 Software, Firmware, and Information Integrity
7	Encryption of Sensitive Data (i.e., PII, PCI, Authenticators): Systems that process PII or other sensitive information shall employ encryption of data while at rest and while in transit. Authenticators (i.e., passwords), PII and PCI are required to be encrypted at rest, in files, and in databases, as applicable. If stored in databases, encryption can be implemented at the field, column, or table level, as appropriate. Ciphers shall be FIPS-approved. If an assessment identifies the system has not address data encryption at rest,	SC-28 Protection of Data at Rest SC2-28(1) Protection of Data at Rest | Cryptographic Protection

#	Showstopper Description	Control Reference
	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.	