Identity Protection Services (IPS)
IPS Requirements Document 1C
in Support of SIN 541990IPS
May 2024

U.S. General Services Administration

[SYSTEMNAME] [ACRONYM]

FIPS 199 Moderate

System Security and Privacy Plan

[Date]

Identity Protection Services (IPS)

SIN 541990IPS Requirements Document 1C

May 2024

FIPS 199 Moderate SSPP - [ACRONYM]

Document Prepared By

Organization Name	
Address Line 1	
Address Line 2	
City, State Zip	

Identity Protection Services (IPS)

SIN 541990IPS Requirements Document 1C

May 2024

FIPS 199 Moderate SSPP - [ACRONYM]

Document Revision History

Date	Comments	Version	Author

Identity Protection Services (IPS)

SIN 541990IPS Requirements Document 1C

May 2024

FIPS 199 Moderate SSPP - [ACRONYM]

Guidance

In addition to the instructions found throughout the template the following guidance is provided to assist personnel in preparing System Security and Privacy Plans (SSPPs) for General Services Administration (GSA) systems. The SSPP is one of the key documents of an information system's security package. Once completed, the SSPP provides detailed descriptions of; (1) all of a system's security control implementations, (2) the system's purpose, function, and operations, including inventories of its components and services, and (3) detailed depictions of the system's data flows, architecture, and authorization boundary.

The GSA Office of the Chief Information Security Officer (OCISO) expectations for specific areas in the SSPP is listed below.

- The latest GSA OCISO SSPP template is to be used by the System Owner (or by proxy) and the system's Information System Security Officer (ISSO) for documenting each assigned information system's security requirements. The completed SSPP must be signed by the following roles for final approval:
    - GSA System Owner
    - GSA ISSO
    - Provider/Vendor ISSO (if applicable)
    - GSA Information System Security Manager (ISSM)
- The System Owner and ISSO must ensure all technologies utilized by the information system are included and described thoroughly in Sections 1-12. Each technology and its purpose supporting the information system should be detailed in the General System Description and System Environment section.
- As part of preparing the SSPP the following documents and subject areas must be completed, reviewed, and approved, or meet the requirements identified.
    - Privacy determination – a Privacy Threshold Assessment, and a Privacy Impact Assessment, if applicable, must accurately identify if Personally Identifiable Information (PII) is in play.
    - Security Categorization – a Federal Information Processing Standards 199 template must be completed and identify all of the information types pertinent to the system and the final security categorization with justification if the FIPS Low, Moderate, or High values have been adjusted.
    - Digital Identity Acceptance Statement (DIAS) – a GSA DIAS must be completed in accordance with the National Institute of Standards and Technology 800-63 series of documents.
    - Security Architecture Review – GSA OCISO's Security Engineering Division (ISE) must have approved the security architecture after reviewing it as described in CIO-IT Security-19-95, "*Security Engineering Architecture Reviews.*"

- The following ATO Showstopper must be fully satisfied with implementation details provided for the controls listed. Additional details are provided in the instructions at the beginning of Section 13 of the SSPP.
  - Multi-factor Authentication for Privileged and User-Level Access - IA-2 (1) and IA-2 (2)
  - Remediation of Critical and High Vulnerabilities – SI-2
  - Remote Code Execution Vulnerabilities – SI-2
  - Usage of End-of-Life Software – SA-22
  - System Architecture Review – PL-8, SA-8
  - Encryption of Sensitive Data (PII, PCI, Authenticators) everywhere – SC-8, SC-8(1), SC-28, SC-28(1)
  - Integration with GSA's Security Stack (Internal Systems)

- Control implementation details in Section 13 of the SSPP must provide detailed implementation descriptions across groups of assets/devices within the security authorization boundary.
- Per GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk*", the Office of the Chief Information Security Officer (OCISO) will review the SSPP to determine if it is complete, consistent, and addresses the security requirements for the information system. Based on the results of the review, the SSPP may require further updating, or may be approved.

Identity Protection Services (IPS)

SIN 541990IPS Requirements Document 1C

May 2024

FIPS 199 Moderate SSPP - [ACRONYM]

Table of Contents

Tables and Figures

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.

Identity Protection Services (IPS)

SIN 541990IPS Requirements Document 1C

May 2024

FIPS 199 Moderate SSPP - [ACRONYM]

Approvals

Instructions: *Signatures are required as part of the Assessment and Authorization (A&A) Process to support the Authorization to Operate (ATO) and annually thereafter. If there is no Vendor ISSO that signature block should be deleted.*

System Owner:

X _____

[Name]
System Owner

Information System Security Officer:

X _____

[Name]
Information System Security Officer

Vendor Information System Security Officer:

X _____

[Name]
Vendor Information System Security Officer

Information System Security Manager:

X _____

[Name]
Information System Security Manager

Identity Protection Services (IPS)

SIN 541990IPS Requirements Document 1C

May 2024

FIPS 199 Moderate SSPP - [ACRONYM]

1 Information System Name

This System Security and Privacy Plan (SSPP) provides an overview of the security requirements for the [SYSTEMNAME] [ACRONYM] and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system.

The security safeguards implemented for the [ACRONYM] meet the policy and control requirements as set forth in this SSP. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table 1-1. Information System Name

Information System Name:	
Information System Abbreviation:	

2 Information System Categorization

The overall FIPS 199 information system security categorization is **Moderate**.

Instructions: *A GSA FIPS 199 Security Categorization document must be completed and submitted as an Attachment to this SSPP. A template is available on the* GSA IT Security Forms and Aids page.

2.1 Information Types

The following table identifies the information types and impact levels that are input, stored, processed, and/or output from the [ACRONYM] environment. The security impact levels for confidentiality, integrity, and availability for each of the information types are expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity, and availability) discussed in NIST SP 800-60 and FIPS 199 (Note: The information types found in NIST SP 800-60, Volumes I and II, Revision 1 are the same information types found in the Federal Enterprise Architecture (FEA) Consolidated Reference Model). Refer to Attachment 2 of this System Security Plan for the detailed FIPS 199 Analysis supporting the summary determinations below.

Table 2-1. Information Types

Information Type	Confidentiality	Integrity	Availability
[First Type]	Choose a level.	Choose a level.	Choose a level.
[Second Type]	Choose a level.	Choose a level.	Choose a level.
[Third Type]	Choose a level.	Choose a level.	Choose a level.

2.2 Potential Impacts of Security Objectives

Based on the information provided above, the potential impacts for each security objective, per FIPS 199, for the [ACRONYM] environment is summarized in the table below.

Table 2-2. Security Objective Impacts

Security Objective	Impact Level
Confidentiality	Choose a level.
Integrity	Choose a level.
Availability	Choose a level.

2.3 Digital Identity Acceptance Statement

Instructions: *A GSA Digital Identity Acceptance Statement document must be completed and submitted as an Attachment to this SSPP. A template is available on the GSA IT Security Forms and Aids page. Record the summary information below based on the completed template.*

Refer to Attachment 3 of this System Security and Privacy Plan for the completed GSA Digital Identity Acceptance Statement form supporting the summary determinations below.

Table 2-3. Digital Identity Acceptance Statement Assurance Level Summary

Assurance Levels	Implemented Assurance Level
Identity Assurance Level (IAL)	Choose a level.
Authentication Assurance Level (AAL)	Choose a level.
Federation Assurance Level (FAL)	Choose a level.

3 Information System Owner

The following individual is identified as the System Owner for this system.

Name	
Title	
Organization	
Address	
Phone Number	
Email Address	

4 Authorizing Official

The Authorizing Official (AO) for this information system is identified below.

Name	

Title	
Organization	
Address	
Phone Number	
Email Address	

5 Other Designated Contacts

The individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

Name	
Title	
Organization	
Address	
Phone Number	
Email Address	

Name	
Title	
Organization	
Address	
Phone Number	
Email Address	

6 Assignment of Security Responsibility

The Information Systems Security Manager (ISSM) has been appointed and is identified below.

Name	
Title	
Organization	
Address	
Phone Number	
Email Address	

The Information Systems Security Officer (ISSO) has been appointed and is identified below.

Name	
Title	

Organization	
Address	
Phone Number	
Email Address	

7 Information System Operational Status

The system is currently in the life-cycle phase noted in the following table.

Table 7-1. System Operational Status

System Operational Status	Status Description
☐ Operational	The system is operating and in production.
☐ Under Development	The system is being designed, developed, or implemented.
☐ Major Modification	The system is undergoing a major change, development, or transition.
☐ Other	Explain:

8 Information System Type

The [ACRONYM] is a [Major Information System/Minor Application/Subsystem].

***Instructions**: The terms General Support System (GSS) and Major Application are no longer used by NIST. Minor Applications/Subsystems are typically authorized to operate under the authorization of a larger Major Application and do not have a standalone authorization to operate. Systems previously considered a GSS or Major Application should be classified as a Major Information System. Contact ISP at ispcompliance@gsa.gov if there are any questions.*

8.1 Systems Providing Controls to [ACRONYM]

***Instructions**: List all systems providing controls, the controls they provide, and identify if it is provided as a Common or Hybrid control. Ensure that the interconnections for systems providing controls are included in the network architecture diagram.*
***Note:** Systems can only inherit controls from systems that have a current ATO.*

The systems identified in the following table provide controls (common or hybrid) to [ACRONYM]. List all systems providing controls, the controls they provide, and identify if it is

provided as a Common or Hybrid control.

Table 8-1. Systems Providing Controls

[Providing System Name] (FISMA System Identifier)	[Providing System Owner]	Control Identifier, Name	Common/ Hybrid
EXAMPLE: GSA Alpha (GSA-A)	*Joe Smith*	*PE-6, Monitoring Physical Access*	*Common*

8.2 Systems Receiving Controls from [ACRONYM]

[ACRONYM] provides the controls (common or hybrid) listed to the systems identified in the following table. List any controls provided to any systems and identify if it is provided as a Common or Hybrid control.

Table 8-2. Systems Receiving Controls

[Receiving System Name] (FISMA System Identifier)	[Receiving System Owner]	Control Identifier, Name	Common/ Hybrid
EXAMPLE: GSA Beta (GSA-B)	*Mark Taylor*	*AC-2, Account Management*	*Hybrid*

9 General System Description

***Instructions**: The general information system description must consist of the following:*

- *How the system is commensurate with the essential characteristics of secure systems defined in NIST SP 800-53 Rev. 5, other applicable NIST guidance and standards, and Federal laws and regulations. In addition, the description shall describe the service model and deployment model.*
- *Convey the who, what, when, where, and how in regards to the system function and purpose across the entire technology stack and all users.*

9.1 Information System Locations

Physically, the [ACRONYM] environment resides at the locations identified below.

Table 9-1. System Locations

Primary
Secondary (if applicable)

9.2 Information System Components and Boundaries

Instructions: *In the space that follows, describe the information system's major components, interconnections, and boundaries in sufficient detail that accurately depicts the authorization boundary for the information system. The desired architecture boundary for an information system should be inclusive of all functions and services necessary to secure, operate, and administer the information system - these include all components and supporting information system components (e.g., logging platform, monitoring solutions, ticketing solutions, vulnerability scanning, authentication solutions, etc.). A system is typically deployed in a logically or physically separated environment situated behind a firewall, with only necessary ingress/egress port openings to facilitate required operations. Integration with assets/device outside of the protected enclave supporting the information system contemplated for an Authorization to Operate (ATO) including but not limited to 1) shared assets, 2) corporate networks, or 3) third party services (e.g., cloud service provider (CSP) offerings) are a function of risk. The latter is allowed if the connecting CSP offering is also Federal Risk and Authorization Management Program (FedRAMP)-authorized. In all cases, integrations with assets/devices outside of the ATO boundary is not guaranteed for approval and reviewed/permitted on a case-by-case basis after a complete understanding of the associated risks. Please ensure that the discussion on boundaries is consistent with the network diagram shown in Section 9.5. For further details, please reference* CIO-IT Security-19-95*, "Security Engineering Architectural Reviews."*

The components of the [ACRONYM] environment can be broken down into the following groups of asset types. The assets are also portrayed in the network diagram in Section 9.5.

The controls described in Section 13 of this document may apply to some or all of these asset types.

Table 9-2. System Assets

Asset Type	Description of Function or Service Provided

9.3 Information System Web Site URL Addresses

Instructions*: List all URLs associated with the information system including the system component; application URL; if it is internal, external, or both; and the multi-factor authentication (MFA) authentication method used. Please specify the tool or technology used to support MFA.*

The following table lists the web site URL addresses for [ACRONYM].

Table 9-3. System URLS

System Component	Application URL	Internal, External, or Both	MFA Authentication Method

9.4 Types of Users

Instructions: *For an External User, please write "Not Applicable" in the Sensitivity Level Column. Please include systems administrators and database administrators as role types. (Include web server administrators, network administrators, and firewall administrators if these individuals have the ability to configure a device or host). Add additional rows if necessary. For MFA Authentication please specify the tool or technology used to support MFA. Personnel who support the system but do not login to the system do not need to be listed.*

All users have their employee status categorized with a sensitivity level in accordance with PS-2. Employees (or contractors) of GSA are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in the table that follows.

Table 9-4. User Roles and Privileges

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed	MFA Authentication Method
Example - Customer Console User	*External*	*NP*	*N/A*	*Application-level access*	*Used to access and interact with application features via GUI*	*UID/PW plus MFA TOTP*
Example - Infrastructure Engineering Team	*Internal*	*P*	*Medium*	*Infra Access*	*Deployment of infrastructure and build automation systems*	*UID/PW plus MFA using Google Authenticator at VPN layer*

Note: User roles typically align with Active Directory, LDAP, Role-based Access Controls (RBAC), NIS, UNIX groups, and/or UNIX netgroups.

Privileged User Access

Instructions: *Provide a brief description of the authentication process for a privileged user. The description should clearly show authentication from an administrative laptop/workstation to the privileged access point or points. This should capture the access for the backend and frontend as applicable. The description should include the technologies (i.e., MFA software, Active Directory, jumpbox, etc.). The description should capture all privileged access points (i.e., shell/remote desktop protocol (rdp) remote sessions, administrative graphical user interface (gui), database, etc.). The description should include all credentials used at all authentication points.*

Non-Privileged User Access

Instructions: *Provide a brief description of the authentication process for a non-privileged user. The description should clearly show authentication from a non-privileged user laptop/workstation to system or application access point. This should capture the access for backend and frontend as applicable. The description should include the technologies (i.e., MFA software, jumpbox, etc.). The description should include all credentials used at all authentication points.*

Vendor Considerations

Instructions: *If a vendor system, include a narrative on how the corporate network is demarcated to the authorization boundary. Also include other measures in place to logically and physically isolate the corporate networks from the ATO boundary.*

9.5 Network Architecture

The following section provides a written description of the network architecture of [ACRONYM].

Instructions: *The architecture diagram must fully and clearly define the authorization boundary through both pictorial diagram(s) and written descriptions.*

Ensure the following elements are incorporated into the architecture diagrams and narratives:

The network architecture must follow the criteria listed in the CIO-IT Security-19-95, "Security Engineering Architectural Reviews." ***The GSA Security Engineering team can provide architectural templates for reference - contact seceng@gsa.gov.***

- *The diagram(s) and narratives should include ALL assets, services, devices, and software, both physical and virtual, which constitute the information system. These shall include all physical and virtual resources. The diagram(s) and narratives should also include any COOP / DR site integrations as well as any test / development environments that are in the boundary.*
- *If shared assets or services are used, including corporate shared services, they must be appropriately defined and documented as a shared service within the ATO boundary of the system or within the corresponding ATO boundary of a relevant, authorized system. All components must be accounted for within an ATO boundary.*

- *If on-premise or cloud services are used to support operation, maintenance, management, security of the services in scope of the ATO, be sure they are reflected in the network architecture with related flows. If integrated with the GSA security stack indicate that integration in the network diagram. Depending on the nature and type of integration and sensitivity of the data, these dependent systems may also need to have an ATO; usage considered for risk acceptance; or, if not risk accepted, potentially removed from the architecture. All SaaS, IaaS or PaaS leveraged that support delivery of the system must have an ATO, approved by GSA or FedRAMP. For public facing systems, integration with external systems including but not limited to other cloud assets via Application Programming Interfaces (APIs) or third-party enablers shall be appropriately secured.*
- *Ensure all authentication points (this includes but is not limited to Amazon Web Services (AWS) console, jump, machine resources, network devices, application, API, enablers, etc. (as applicable)), are defined. 2FA should be for privileged, non-privileged and/or Internet accessible logins within this system (for both customers and vendor staff). At FIPS 199 Moderate and up, all authentications shall be 2FA; privileged authentication is required to be MFA for all FIPS impact levels.*
- *The system boundary contains all components, devices, services, communication paths (VPNs, API calls, etc.). Diagram(s) should be sufficiently detailed and identify flows with source/destination, ports/protocols, or whether the related traffic is encrypted or not. References to ports/protocols table(s) are acceptable (for large sets of ports). Please be sure the tables identifying ports reflect whether they are encrypted or not. Tables should easily track to the architecture diagram.*
- *All access control mechanisms, such as firewalls, router ACLs, subnets, proxies, and cloud-based analogs such as firewalls and network access controls configurations shall be fully documented in terms of specific access control rules, specifying source, destination, protocol, and other relevant attributes, as necessary.*
- *The diagram must include a predominant border drawn around all system components and services included in the authorization boundary. Separate borders around protected enclaves, subnets, and DMZs are also advisable.*

The following architectural diagram provides a visual depiction of the major hardware components of the [ACRONYM].

Instructions: *Insert network diagram here.*

Figure 9-1. Network Diagram

10 System Environment

Instructions**: In the space that follows, describe the technical system environment and document the architecture requirements identified within Sections 9.1 through 9.3 of this document. Include information about all system environments that are used, (e.g., production, test, staging or QA environments). Ensure that the proposed software stack utilizes current and supported versions. T**he software stack, including operating system, application, database, etc. must be configured and hardened in accordance with** GSA technical guidelines**, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as deemed appropriate by the GSA AO.

The mechanisms for creating, storing, distributing, and signing any encryption keys or certificates in the system shall be fully documented in the security architecture. Additionally, all keys and certificates generated shall be reposed in a manner that assures Business Continuity Plan (BCP), Disaster Recovery (DR) and Continuity of Operations (COOP) consistent with NIST requirement per impact FIPS 199 impact level. For further details, see the GSA Key Management Guide.

*****Systems that process Personally Identifiable Information (PII), Payment Card Industry (PCI) data, Authenticators (e.g., passwords, tokens, keys, certificates, hashes, etc.), and other sensitive data (as determined by the AO, it shall be encrypted everywhere (i.e., at file level, database level, at rest, and in transit). For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption.*****

Encryption algorithms shall be FIPS-approved with FIPS-validated encryption modules.
If transmitted, utilize secure protocols (e.g., TLS 1.1 and up), Hypertext Transfer Protocol (HTTP) Strict Transport Security (HSTS) and HTTP Secure (HTTPS) only.

- Digital signature encryption algorithms
- Block cypher encryption algorithms
- Binding Operational Directive 18-01

10.1 Asset Inventory

***Instructions**: For addressing the system's virtual and physical inventory. If the system inventory is maintained via OCISO SecOps shared Google inventory document; select the '(link)' right-click and select Hyperlink. Add the information system's shared Google inventory document URL as the 'Address' in the hyperlink. Once completed, remove the second statement 'The following table identifies the virtual and physical components of the [ACRONYM]' and Table 10-1.*

If the system's inventory is not maintained within an OCISO SecOps shared Google inventory document. Remove the first statement 'The following link lists the virtual and physical components of the [ACRONYM] (link).' and document the system's inventory in the provided table.

The following link lists the virtual and physical components of the [ACRONYM] (link).

The following table identifies the virtual and physical components of the [ACRONYM].

Table 10-1. Asset Physical and Virtual Components

Component Name	OS/Make	Operational Environment	Location (Physical or Virtual)
Appname-app-1.gsa.gov EXAMPLE	*MS Windows 2019*	*Production*	*Virtual (AWS, us-east-1)*

10.2 External Services

Instructions: *In the table below, fill out the applicable details for any external services that integrate with the system. If non applicable, just state there are no external integrations. Use the following bullet list as guidance to accurately populate the services table for each external connection proposed for integration with the information system considered for Authorization to Operate (ATO) consideration.*

- *System Name: Name of external system (SaaS or Corporate Service, etc.)*
- *Connection Type: Describe the type of connection flow as unidirectional incoming, unidirectional outgoing, bi-directional, or none. (Incoming, Outgoing, Bi-directional, none)*
- *Data Description: Provide a description of the data content and classification associated with the connection. Does the data contain government data, PII, CUI, etc.? (Yes / No, (Gov. Data, CUI, Proprietary, etc.)).*
- *Data Sensitivity: Describe the sensitivity of the data (Low, Moderate, High). Include a brief description of how this data was categorized (i.e., FIPS 199, internal corporate processes, etc.).*
- *Level of Vendor Dependency: Describe the level of dependency (Low, Moderate, High) on the vendor regarding configuration of support and security control implementation. Include decision logic and how difficult it would be to migrate to an alternative if not approved for use.*
- *Alternative Exists: Does an alternate service exists which performs the same functionality? (Yes / No) If yes, describe the alternate service.*
- *Is API over HTTPS: (Yes / No).*
- *API Connection Security: (OAuth 2.0, HTTP, Digital Certificates/ TLS Client, SAML, HMAC)*
- *API Connection Type: It is important to recognize that vendors are inconsistent in their use of the term "API key". It is often used as a stand-in for "tokens", "codes", "customer identifiers" depending on the product and usage. The following bullets cover the scenarios:*
  - *Inbound: An external system uses an API key to communicate with the CSP Infrastructure/Platform API to obtain information about or data from the vendor resources. This scenario is only applicable to external systems requiring connectivity inbound to the CSP.*

– Outbound: A CSP system uses an integration token to communicate with an external system. Sometimes the vendors refer to these as "API Keys", but this is not an accurate description because they are simply a customer identifier.

– Sync: An external system uses an API key to communicate with another external system

- *Authentication and Authorization: Describe how the service authenticates to the system. For example: User ID and password, Secure Shell (SSH) key, token, SAML federation, etc. (UID, PW, Key, Token, Federated, User ID + token, etc.).*
- *MFA: Does the service connection require MFA? (Yes / No) If yes, which MFA vendor is being used?*
- *Role Based Access Control: Is Role-based access control implemented for authentication? (Yes / No)*
- *Audit Logs Available: Does the external system provide the capability to generate audit logs that are available to the consumer? (Yes / No)*
- *Encryption in Transit: Is data encrypted during transit (Yes / No)? If yes, what type of encryption is used (i.e., TLS 1.2).*
- *Encryption in Storage: Is the data encrypted at rest (Yes / No). If yes, what type of encryption is being used (i.e. AES 256)? Are the encryption modules FIPS Validated?*

Note: *Make a copy of the table and populate for each external service*

The following table(s) identifies the external services supporting [ACRONYM].

Table 10-2. External Service

Service Element	Response
System Name	
Connection Type	
Data Description	
Data Sensitivity	
Level of Vendor Dependency	
Alternative Exists	
Is API over HTTPS?	
API Connection Security	
API Connection Type	
Authentication and Authorization	
MFA	
Role-based Access Control	
Audit Logs Available	
Encryption in Transit	
Encryption in Storage	

10.3 Software Inventory

Instructions: *Populate the following table with the major Operating Systems and Applications within the system boundary. The full name of the software should be used (i.e., Red Hat 6 vs Linux.)*

The following table lists the principle software components (e.g., operating system, database, web software, etc.) for [ACRONYM].

Table 10-3. Software Components

Software Component/Name	Function	Version	Patch Level	Virtual (Yes / No)

10.4 Data Flow

***Instructions**: In this section describe the flow of data in and out of system boundaries and insert a data flow diagram. If necessary, include multiple data flow diagrams.*
Ensure the following elements are incorporated into the data flow diagrams and narratives:

- *Indicate source and destination of data (Is communication crossing DMZ's, subnets, to another authorization boundary, external service, internet, etc. Also include whether it is one way inbound, one way outbound, or bi-directional).*
- *Identify the ports and protocols planned for use and whether the flows are encrypted.*
- *Note any access control mechanisms in place to restrict the flow of authorized traffic between defined and approved endpoints.*
- *Clearly identify anywhere Federal data is to be processed, stored, or transmitted*
- *Document any data flow through approved external or internal Continuous Integration systems (CI) and code repositories in flow narratives and SSPP diagrams. Clearly identify data flows for privileged, non-privileged, and customer access.*
- *Include data flows associated with BOTs, as applicable, to ensure data flows used by BOTS are depicted.*

The Data Flow Diagram (DFD) below maps out the flow of information traveling within an information system and between information systems.

Instructions: Insert data flow diagram here.

Figure 10-1. Data Flow Diagram

10.5 System Data Nature

***Instructions**: Include a narrative on the nature of the data being stored and processed in the system. Ensure the following are incorporated into the narrative:*

- *The nature and type of data (regardless of if it is PII, PCI, or Authenticators).*
- *Is the data PII, PCI, or Authenticators? If so, how is it encrypted at a file level?*

- *Include details where the encryption keys are stored.*
- *Include details on how the keys are managed and protected.*
- *Include the algorithm being used to encrypt the data along with details on FIPS level.*

10.6 Ports, Protocols and Services

***Instructions**: In the column labeled "Purpose" indicate the purpose for the service (e.g., system logging, HTTP redirector, load balancing). This table should be consistent with CM-6. Add more rows as needed. Ensure any ports used to support BOT functions are included and the support of BOTs is explicitly stated in Purpose.*

The table below lists the Ports, Protocols, and Services enabled in this information system. TCP ports are indicated with a T and UDP ports are indicated with a U.

Table 10-4. Ports, Protocols, and Services

Direction (Inbound, Outbound, or Bi-Directional)	Boundary Crossings (Y/N)	Source	Destination	Ports (T or U)	Protocols	Services	Purpose	Encrypted (Y/N)	Data Sensitivity

***Instructions**: System teams using DevOps/DevSecOps practices (Section 10.8), containers for deployment of their application (Section 10.9), or AWS cloud-based platforms (Section 10.10) must complete the identified section(s) to ensure their environment, practices, and tools are understood in the context of securing the system and is operation and maintenance. If an entire section (10.8, 10.9, 10.10) is not used the entire section should be deleted.*

10.7 Transition to IPv6

***Instructions:** Describe how the system will transition to IPv6 as required in OMB Memo 21-07, "Completing the Transition to Internet Protocol Version 6 (1Pv6). and in accordance with GSA CIO Instructional Letter IL-21-01, "Internet Protocol Version 6 (IPv6) Policy," and guidance from the GSA IPv6 Integrated Project Team (IPT).*

10.8 DevOps/DevSecOps Management

10.8.1 Code Version Control and Code Management

***Instructions**: Describe how code is stored and maintained, the code repository branching strategy, the code review process, and the unit/integration test coverage and deployment strategy. Describe how code is tested, verified, and committed, including pre-commit checks, linting and code-scanning checks in the developer's IDE. Identify the workflow steps and how code changes are linked to work items and change requests.*

10.8.2 Infrastructure-As-Code (IAC) Implementation

***Instructions**: Describe how the infrastructure is maintained. Explain the steps taken to codify the infrastructure, how lower and higher environments are deployed from the same source code, the usage of a CI/CD pipeline with regard to infrastructure-as-code implementation, security checks performed for misconfiguration and errors before IAC deployment.*

10.8.3 Pipeline Design

***Instructions**: Describe the pipeline used to deliver features. How is the CI environment isolated and secured. Explain the steps taken to include infrastructure and application code in the CI pipeline. Describe the process for performing blue-green deployments, if applicable.*

10.8.4 Code Scanning

***Instructions**: Describe how code is scanned for security issues during development. How are linting tools used? Explain how the code is checked for secrets. Describe the process for scanning 3rd party libraries and performing static analysis.*

10.8.5 Dependency Scanning

***Instructions**: Describe the process for running dependency scans and at what stages in development they are run. If there are vulnerabilities found, what is the process for handling these vulnerabilities? Describe the process of scanning dependency artifacts.*

10.8.6 Image Management

***Instructions**: Explain the process for building, updating and republishing Amazon Machine Images (AMIs) or equivalent images. Describe what base operating systems image, packages and software are used to build images. What is the retention policy for images? Explain steps in image building, security check, and validation for gated release of images. Explain the process/permission control for creation, sharing and validation/release of approved images or Gold images.*

10.8.7 Secret and Key Management

***Instructions**: Describe secrets are centralized and how hard coded and embedded secrets are eliminated. What is the process for rotating and auditing secrets? Describe the process for monitoring and generating alerts on improper uses/access of keys and secrets.*

10.8.8 Artifact Management

***Instructions**: Describe the process for maintaining artifacts. Describe scanning artifacts and how often this is performed. What authentication and authorization mechanisms are used to access artifact management tools? Describe the process for monitoring and notification of outdated libraries found in artifacts.*

10.8.9 Code Change and Release Management

***Instructions**: Describe how the process for handling all code changes and release management is standardized. Describe the sequence of steps or activities used for change management. Describe automation or tools used to improve security, speed and efficiency during code change and release management. What is the security review and approval process of each change/release?*

10.8.10 Serverless Design (if applicable)

***Instructions**: Describe the microservice-based architecture including API and API security. Describe the serverless functions network security model including the perimeter. Describe the code review, scanning, and the dependency scanning tools chain and processes.*

10.9 Container-Based Workload Management

10.9.1 Container Image Build and Management

***Instructions**: Describe how images for Containers are built, how a Continuous Integration/Continuous Delivery (CI/CD) pipeline is used to build and release container images, describe the steps involved in the CI/CD pipeline, describe security checks and tools used in the pipeline and describe how container images are protected.*

10.9.2 Container Image Scanning

***Instructions**: Describe how container images are scanned for security vulnerabilities. Which tools are used for container vulnerability scanning? How often are scans performed and how are images in the CI/CD pipeline scanned. Describe vulnerabilities identified in containers are remediated. Note: GSA OCISO requires the use of Prisma Cloud for internal systems at GSA.*

10.9.3 Container Image Registry

***Instructions**: Describe which container registry is used (e.g., Amazon Elastic Container Registry [ECR], Docker Hub.). Describe what functions of the container registry are used. Describe if it is self-hosted or a managed service provided by a CSP. If it is an external provider, is the service FedRAMP compliant or approved by GSA? Describe the access control mechanisms and security control measures in place for the Container Registry.*

10.9.4 Dockerfile Usage

***Instructions**: Describe how Docker images are developed. Are the Docker images built from scratch or are base images from an external source used? If it is from source, explain any code quality mechanisms used, such as a linting tool. If images from an external source are used, explain the mechanisms in place to ensure this image can be trusted.*

10.9.5 Logs and Log Integration from Containers

***Instructions**: Describe how logs generated from containers are aggregated in a central log repository. Explain the tooling used to analyze logs and trigger action if needed.*

10.9.6 Hardening of Container Infrastructure

***Instructions**: Describe which Container Infrastructure is used. Is a fully managed or semi-managed container platform from a CSP used? Is the service FedRAMP compliant or approved by GSA? Has the cluster been hardened to security guidelines provided by Center for Internet*

Security (CIS) benchmarks or other similar benchmark? Are underlying virtual machines run in the cluster hardened?

10.9.7 Privilege Management in Cluster and Containers

***Instructions**: Describe how least privileges are applied to users or administrators that need access to a cluster. Is Role-Based Access Control (RBAC) used? Is a non-root user used to run the application with the container? Please explain the approach used to ensure least privilege both for the CSP and containers.*

10.9.8 Container Network Security

***Instructions**: Describe how network security control is implemented for communication between cluster resources. Describe the network topology for the container infrastructure? How is network traffic monitored and restricted between containers? How is network traffic isolated from containers to managed services such as a Database or a Caching cluster? Explain the use of any additional tools for container network security and segmentation in a multi-application multi-tenant/multi-application environment.*

10.9.9 Container Orchestration (Elastic Container Service (ECS), Elastic Kubernetes Service (EKS), Fargate, Kubernetes, etc.)

***Instructions**: Describe the Container Orchestrator used. Is it supported or managed by a vendor? Is it FedRAMP compliant or GSA OCISO approved? Has the Orchestrator been hardened to security guidelines provided by the CIS benchmarks or other similar benchmarks?*

10.9.10 Monitoring and Alerting

***Instructions**: Describe how monitoring on Containerized applications is performed. Does the monitoring provide a holistic view across Containers, Cluster, Host machines, communication and telemetry between containers? Describe how notifications are received when monitoring finds issues of interest.*

10.10 AWS Management

10.10.1 List of AWS Services Used

***Instructions**: List AWS services used in the system boundary in the table below.*

Table 10-5. AWS Services

AWS Service Name	Approval Status (FedRAMP and/or OCISO Approved)	Brief Description of Use(s)

10.10.2 Identity and Access Control Management

***Instructions**: Describe the identity and access control design for AWS platform level access. It should include technology used for authentication and authorization such as federation, single sign-on and/or identity access management (IAM). Describe how MFA is achieved. Provide details on authentication and authorization for API access, how is MFA achieved for interactive API or command line access. Describe how least privilege is being implemented, what methods and tools are being utilized to develop and assign IAM policies to meet least privilege requirements.*

10.10.3 Separation of Workloads

***Instructions**: Describe the AWS account strategy for defining separation of workloads (e.g., Dev, Test, Prod are separate AWS Accounts). Describe the network segregation in place between these environments (e.g., All AWS Accounts are logically separated from each other with no mesh network or connectivity between them.). Describe how new code, features, enhancements, and fixes are promoted from lower environments to production environments.*

10.10.4 Cloud Network Design

***Instructions**: Describe the network's high availability strategy. For example:*

- *Web server fleet is behind elastic load balancers*
- *Utilizing multiple FedRAMP authorized regions*
- *Utilizing multiple availability zones*
- *Public websites are behind Cloudfront*
- *Utilizing Web Application Firewalls to mitigate exploits and denial of service attacks*
- *Utilizing public and private subnets*
- *Utilizing private endpoints so traffic does not traverse public internet if it can stay internal to*

AWS.

10.10.5 Network Security and Microsegmentation

***Instructions**: Describe the network's security group and network access control list (NACL) strategy. (e.g., wide permissions are not in place and each Security Group only allows the traffic it requires, 0.0.0.0/0 rules are not in place).*

10.10.6 Data Encryption in Transit

***Instructions**: Describe the network's encryption in transit strategy (e.g., Secure Sockets Layer/Transport Layer Security [SSL/TLS] is in use for public web servers, the SSL connections are terminated on the hosts instead of the load balancer to provide true end to end encryption, uses of other application layer encryption technology such as SSH, Secure File Transfer Protocol (SFTP), etc.).*

10.10.7 Data Encryption at Rest

***Instructions**: Describe the encryption at rest strategy. (e.g., all Elastic Block Store (EBS) Drives and Simple Storage Service (S3) Buckets have AES-256 Encryption Enabled, Relational Database Service (RDS) databases have force encryption parameters enabled, Simple Notification Service (SNS) Topics have encryption enabled, data encrypted in field, table, column level to protect sensitive data stored within the database, files and logs with sensitive information are encrypted before placing in buckets and file systems).*

10.10.8 S3 Bucket Security

***Instructions**: Describe the S3 Bucket Security Strategy. (e.g., all S3 Buckets have AES-256 encryption enabled, all S3 Buckets do not have public access enabled or is explicitly blocked from being public, least privilege access in place for each bucket, AWS config rules are monitoring changes to S3 Bucket posture and changes to provide operational assurance, no static websites are in use, Amazon Macie is enabled to monitor for sensitive information stored in S3).*

10.10.9 Key Management Service (KMS) Key Monitoring and Governance

***Instructions**: Describe the KMS and Key Management Strategy. (e.g., all AWS encryptable services that can utilize KMS Keys have KMS Keys in place, IAM policies are in place that only allow specific users to manage keys for such services, IAM policies are applied granularly per KMS Key, KMS Keys are rotated every 60 days, KMS activity is monitored in CloudTrail).*

10.10.10 Governance and Management of AWS Accounts

***Instructions**: Describe the AWS account provisioning and decommissioning strategy for all AWS accounts (e.g., production, test, development). Describe any governance, guardrails, or security inheritance achieved by using centralized AWS account provisioning, or by using AWS services such as AWS organization, Service Control Policies (SCPs), AWS Single Sign-On (SSO).*

10.10.11 Uses of Cloud Native Security Services

***Instructions**: Describe the Cloud Native Security Services utilized and how they are implemented. (e.g., Security Hub is enabled to validate meeting CIS Benchmarks, Guard Duty is enabled with flowlog monitoring, AWS Web Application Firewalls (WAFs) are in front of public Elastic Compute Cloud (EC2) servers, AWS Secret Manager is used for key/secret rotation, AWS Macie is enabled to identify and protect sensitive data in S3).*

10.10.12 Continuous Monitoring and Assessment of AWS Security Posture

***Instructions**: Describe how baseline AWS Security is implemented and monitored. (e.g., AWS Security Hub is enabled and meets CIS Benchmarks, AWS Config is used for continuous checks against best practices and deviation, third-party tools are used for continuous assessment of cloud posture, CloudTrail and CloudWatch logs are configured and shipped to the GSA Elastisearch, Logstash, Kibana (ELK) Platform, automated alerts are in place for sensitive changes, Security Hub is periodically reviewed to validate compliance against CIS).*

11 System Interconnections

***Instructions**: List data covering all interconnected systems in the two tables in this section as described below. Add additional rows as needed. A system interconnection is the direct connection of two or more IT systems for the purpose of sharing information resources (data or services). An ISA or MOU is required between systems that share data that are owned or operated by different organizations and where data is transmitted between each system. All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be approved by the GSA CISO.*

Table 11-1 documents high level information for ALL system interconnections. If an ISA/MOU is not required place N/A in both the Agreement Type and Date of Agreement columns.

Table 11-2 documents detailed information for ALL system interconnections. This data is vital to understanding the nature of the interconnection between the systems. Provide sufficient information (e.g., System Name, component IP address and interface identifier) connecting to this system. Name the organization and the POC for the external system. For Connection Security indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number.

Table 11-1. System Interconnections

System Name	Organization	Type of System (Major Information System/ Minor Application/ Subsystem)	Agreement Type (ISA, MOU)	Date of Agreement	FIPS 199 Security Category of System	A&A Status of System	Name and Title of AO

Table 11-2. Connection Details of Interconnected Systems

System Name	Organization	Point of Contact and Phone Number	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)	Data Direction (incoming, outgoing, or both)	Information Being Transmitted	Ports or Circuit #

Note: *For system interconnections with an ISA/MOU, additional information regarding connection may be found in the associated ISA/MOU.*

12 Applicable Laws and Regulations

See Appendix B, References.

13 Minimum Security Controls

Minimum security controls for the [ACRONYM] environment are contained in the following sections.

Instructions: *The control implementation must meet (or exceed) the GSA provided control parameters and/or requirements to fully implement the control and enhancements. As an example, if the requirement states a semiannual frequency, the SSPP must specifically state the frequency is semiannual to meet the requirement or more frequently (if the system exceeds the requirement).*

The network access controls shall be implemented in a least-permissive manner, assuring that only authorized and essential network communication occurs between elements of the system and across system boundaries.

For Security Control CA-7, the implementation statement must align with GSA CIO-IT Security-08-39, "Management Implementation Plan" and CIO-IT Security-12-66, "ISCM Strategy and OA Program."

Guidance for Implementation Status:
If the control or enhancement implementation status is "Planned" a description of the time-bound plan commensurate documented in the control implementation description. Any critical items that will not be fully satisfied by an ATO will need to be reviewed and approved by the GSA CISO and AO Additionally, if a finding remains as an open item in the POA&M, the security control must be changed in the SSPP to "Planned," the bottom of the implementation statement must have the POA&M ID in bold letters, and the recommendation statement from the SAR.

If the control or enhancement implementation status is "Not Applicable," a clear description of the justification and itemization of any evidentiary artifacts of compensating controls supporting the position must be provided in the SSPP.

Guidance for Control Origination:
For Hybrid controls, an information system and customer section (if applicable) must exist to properly describe the control implementation responsibility in detail. Component agencies are responsible for separately assessing and authorizing controls relating to Hybrid controls where they have implementation responsibility. The SSPP must describe how the information system has implemented all facets of every control requirement. Sub-requirements to respond to within the control are often provided as lists itemized either by letter, number, or bullets. System Owners and ISSOs are advised that the structure of implementation detail should be similar to

the control's compartmentalization. Preparers of the SSPP may add additional Hybrid control selections if the system inherits portions of a control from more than one system.

Guidance for Describing Control Implementation:
Document the security control implementation, in accordance with GSA implementation guidance in the GSA IT Security Procedural Guides provided by the ISSO. For controls with one or more enhancements, each enhancement and all sub-requirements therein must be addressed.

Controls discussions are typically broken out into three response types:

- *Discussions by Asset/Device Type (e.g., CM-6 Configuration hardening for servers, databases, web servers, etc.). This may include networking devices, SAN/NAS, servers, hypervisors, portals, APIs, etc. This is especially important for controls in the technical and operational families including but not limited to the AC, AU, CM, IA, SA, SC, and SI control families. Within these families, the following controls and all associated enhancements (not separately identified in the list below) are likely to be impacted and require detailed implementation descriptions across asset/device types. (This list is a sample and not comprehensive): AC-2, AC-3, AU-2, CM-2, CM-6, IA-2, SC-7, SC-28(1)*
- *Discussion by Access/Identification/Authentication Method (e.g., authentication to machines, jump solutions, web portals, databases, networking gear, etc.) (This list is a sample and not comprehensive): IA-2, IA-2(1), IA-2(2), IA-2(12), SC-10, SC-13*
- *Common control discussion that applies consistently to all assets and devices in the ATO boundary (e.g., Training, personnel security, physical security, etc.).*

***Note:** there could be situations where controls could be documented as either component or common, such as AC-6 or AU-6.*

Be sure to:
Write to each control part (Part a, Part b, Part c, etc.)

Define the "who, what, when, where and how" each control is in place. Do not just reiterate the security control requirements

Address the entire IT stack (i.e., each platform – Windows, Unix/Linux, Database, Web, Network, etc.)

Ensure each GSA Defined Value as shown in the GSA Control Tailoring Workbook, also known as Organization Defined Parameter (ODP), is being met. Ensure that all parameters identified for the Service/Staff Office or Contractor to define with GSA CISO and AO approval are defined.

The following 3-year Authorization to Operate (ATO) and Ongoing Authorization (OA) show stopper security controls have been identified by the GSA CISO.

#		
1	Multi-Factor Authentication (MFA) for Privileged & User-level access: All systems shall utilize a GSA-approved multi-factor authentication mechanism for both privileged and non-privileged user authentication. Further, systems leveraging certificate-based authentication shall not be downgraded to only username and password authentication. Per NIST 800-63B, "*Digital Identity Guidelines, Authentication and Lifecycle Management*," MFA 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 on GFE is allowed based on a risk analysis. MFA 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) | Multifactor Authentication to Privileged Accounts IA-2 (2) Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts
2	Critical and High vulnerabilities: GSA requires ongoing remediation actions including patching, updating and upgrading out of date components, addressing known vulnerabilities, completing POA&Ms, maintaining secure configurations of components. If an assessment identifies ongoing remediation actions that are not being addressed, then the system will not be approved for a 3-year ATO or OA, until the associated risks are mitigated.	SI-2 Flaw Remediation
3	Remote Code Execution (RCE) Vulnerabilities: RCE vulnerabilities can be exploited if user input is injected into a File or a String and executed (evaluated) by the programming language's parser. RCE vulnerabilities must be remediated, regardless of the RCE system impact level identified. 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
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:	PL-8 Security and Privacy

#	Showstopper Description	Control Reference
	CIO-IT Security-19-95, "Security Engineering Architectural Reviews" identifies the OCISO Security Engineering (ISE) system evaluation requirements. If an assessment identifies an ISE system review has not been completed for the system, then the system will not be approved for a 3-year ATO or OA, until one is completed.	Architecture SA-8 Security and Privacy Engineering Principles
6	Integration with GSA's Security Stack (Internal Systems): System integration includes; • Sending logs to GSA's central Enterprise Logging Platform (ELP) to support information system monitoring. • Using GSA's configuration setting monitoring tools (BigFix, MasS360). • Installing GSA's tool for whitelisting/blacklisting and restricting user installation of software (Bit9). • Using GSA's scanning tools to identify vulnerabilities (e.g., Tenable Security Center (TSC), NetSparker). • Using GSA's antivirus and malicious code protection tools (e.g., Cylance AV, FireEye). • Using GSA's inventory management tools (e.g., BigFix, ServiceNow, Forescout/SecureConnector, MaaS260) to monitor assets. **Note:** Tools referenced above relate to GSA's internal infrastructure and systems those tools can be integrated with; GSA cloud environments (e.g., FCS, GRACE) may vary. 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.	Additional details on GSA's security stack can be found in this Google Sheet. GSA ISCM Enterprise Security Management Tools
7	Encryption of Sensitive Data (i.e., PII, PCI, Authenticators): **Systems that process Personally Identifiable Information (PII), Payment Card Industry (PCI) data, Authenticators (e.g., passwords, tokens, keys, certificates, hashes, etc.), and other sensitive data as determined by the AO, shall encrypt that data everywhere (i.e., at file level, database level, at rest, and in transit. For databases, encryption of the whole database, table, column, or field levels is acceptable, as appropriate. Other methods including, but not limited to, application encryption or tokenization is also acceptable. For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption.** If an assessment identifies the system has not addressed data encryption based upon the specific system's data protection requirements, then the system will not be approved for a 3-year ATO or OA, until the deployment requirements have been completed.	SC-8 Transmission Confidentiality and Integrity SC-8(1) Transmission Confidentiality and Integrity | Cryptographic Protection SC-28 Protection of Information at Rest SC-28 (1) Protection of Information at Rest | Cryptographic Protection

#	Showstopper Description	Control Reference
	Encryption algorithms and modules shall be FIPS 140-2/140-3[1], "*Security Requirements for Cryptographic Modules*," validated. ○ Digital signature encryption algorithms ○ Block cypher encryption algorithms ○ Secure hashing algorithms For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption. Internet accessible Websites shall implement HTTPS Only with HTTP Strict Transport Security (HSTS), have no weak ciphers, have no weak protocols, and preload .gov domains. (see Binding Operational Directive (BOD) 18-01, Enhance Email and Web Security). SSL/TLS implementations shall align with CIO-IT Security-14-69, *"SSL/TLS Implementation."*	

[1] NIST has issued FIPS 140-3, FIPS 140-2 modules are still being validated and will be accepted through September 22, 2026. For additional information see the NIST cryptographic module validation program web page.

Guidance for Final Marrying of the SSPP with the SAR and Plan Action Statements.

Update the SSPP based on each procedural SAR finding (do not include technical vulnerabilities (scan findings) identified). The deficiency should be documented within each applicable security control's implementation status. For example, the following SAR finding exists: CP-4 CP Testing was not conducted for FY20.

The ISSO would then scroll down to the CP-4 control within the SSPP and under the subcontrol "a" which corresponds to conducting CP testing on an annual basis; the ISSO would then include the following verbiage under the documented implementation status:

FY20 Assessment Finding:

CP Testing was not conducted for FY20.

In addition, the implementation status checkbox must also be modified to "Partially Implemented" or "Planned."

13.1 Access Control

13.1.1 AC-1: Policy and Procedures

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

AC-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation	

AC-1	Control Summary Information
☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Access Control CIO-IT Security-01-07 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-1 Describe how the control is implemented.	
Part a	1. The GSA access control policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding access control for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Access control procedures are documented in CIO-IT Security-01-07, "IT Security Procedural Guide: Access Control." This guide is disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-01-07 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.1.2 AC-2: Account Management

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;
b. Assign account managers;
c. Require [*GSA S/SO or Contractor recommended prerequisites and criteria (based on defined user role(s) matrix in GSA SSPP Template Section 9: Types of Users) as approved by the CISO and AO*] for group and role membership;
d. Specify:
    1. Authorized users of the system;
    2. Group and role membership; and

3. Access authorizations (i.e., privileges) and [*the following attributes as defined in the user role(s) matrix in GSA SSPP Template Section 9: Types of Users) Internal or External; Privileged (P), Non-Privileged (NP), or No Logical Access (NLA); Sensitivity Level; Authorized Privileges; Functions Performed; MFA Authentication Method*] for each account;

e. Require approvals by [*designated account managers as specified in AC-2.b*] for requests to create accounts;
f. Create, enable, modify, disable, and remove accounts in accordance with [*CIO-IT Security-01-01, Identification and Authentication, CIO-IT Security-01-07, Access Control, and GSA-defined procedures or conditions (as applicable)*];
g. Monitor the use of accounts;
h. Notify account managers and [*System Owner, System/Network Administrator, and/or ISSO*] within:
   1. [*14 days*] when accounts are no longer required;
   2. [*14 days*] when users are terminated or transferred; and
   3. [*14 days*] when system usage or need-to-know changes for an individual;
i. Authorize access to the system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. [*Role privileges identified in GSA SSPP Section 9: Types of Users*];
j. Review accounts for compliance with account management requirements [*annually*];
k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes.

AC-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-2 Describe how the control is implemented.	

AC-2	Control Summary Information
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	

AC-2	Control Summary Information
Part k	
Part l	

13.1.3 AC-2 (1): Account Management | Automated System Account Management

Support the management of system accounts using [*GSA S/SO or Contractor recommended automated mechanisms as approved by the GSA CISO and AO*]

AC-2 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-2 (1) Describe how the control is implemented.	

13.1.4 AC-2 (2): Account Management | Automated Temporary and Emergency Account Management

Automatically [*disables*] temporary and emergency accounts after [*no more than 90 days*].

AC-2 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented	

AC-2 (2)	Control Enhancement Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-2 (2) Describe how the control is implemented.	

13.1.5 AC-2 (3): Account Management | Disable Accounts

Disable accounts within [*30 days*] when the accounts:
(a) Have expired;
(b) Are no longer associated with a user or individual;
(c) Are in violation of organizational policy; or
(d) Have been inactive for [*30 days*].

AC-2 (3)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-2 (3) Describe how the control is implemented.	

AC-2 (3)	Control Summary Information
Part a	
Part b	
Part c	
Part d	

13.1.6 AC-2 (4): Account Management | Automated Audit Actions

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AC-2 (4)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-2 (4) Describe how the control is implemented.	

13.1.7 AC-2 (5): Account Management | Inactivity Logout

Require that users log out when [they have completed their workday].

AC-2 (5)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-2 (5) Describe how the control is implemented.	

13.1.8 AC-2 (6): Account Management | Dynamic Privilege Management

Implement [*dynamic privilege management capabilities provided by enterprise endpoint and network security tools*].

AC-2 (6)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

AC-2 (6)	Control Summary Information
AC-2 (6) Describe how the control is implemented.	

13.1.9 AC-2 (13): Account Management | Disable Accounts for High-Risk Individuals

Disables accounts of individuals within [*24 hours*] of discovery of [*account compromise relating to an incident or Insider Threat event (per the OMA Insider Threat Program) as directed by the GSA CISO, AO, and/or GSA Incident Response Team]*.

AC-2 (13)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-2 (13) Describe how the control is implemented.	

13.1.10 AC-3: Access Enforcement

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented	

AC-3	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-3 Describe how the control is implemented.	

13.1.11 AC-3 (14): Access Enforcement | Individual Access

Provide [*a self service mechanism or use GSA's Privacy Act Request for Access process*] to enable individuals to have access to the following elements of their personally identifiable information: [*as defined in the GSA PII Rules Matrix*].

Note: Only applicable if PII is stored, processed, or transmitted by the system.

AC-3 (14)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-3 (14) Describe how the control is implemented.	

AC-3 (14)	Control Summary Information

13.1.12 AC-4: Information Flow Enforcement

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [*Web Service Security (WS Security), WS-Security Policy, WS Trust, WS Policy Framework, Security Assertion Markup Language (SAML), extensible Access Control Markup Language (XACML)*].

AC-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-4 Describe how the control is implemented.	

13.1.13 AC-5: Separation of Duties

a. Identify and document [*GSA S/SO or Contractor recommended duties of individuals, based on roles and responsibilities, to be approved by the GSA CISO and AO*];
b. Define system access authorizations to support separation of duties.

AC-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented	

AC-5	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-5 Describe how the control is implemented.	
Part a	
Part b	

13.1.14 AC-6: Least Privilege

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AC-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-6 Describe how the control is implemented.	

AC-6	Control Summary Information

13.1.15 AC-6 (1): Least Privilege | Authorize Access to Security Functions

Authorize access for [*any individual or role*] to:

(a) [*GSA S/SO or Contractor recommended security functions (deployed in hardware, software, and firmware) approved by the GSA CISO and AO*]; and

(b) [*Security-relevant information as approved by the GSA CISO and AO*].

AC-6 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-6 (1) Describe how the control is implemented.	

13.1.16 AC-6 (2): Least Privilege | Non-Privileged Access for Non-Security Functions

Require that users of system accounts (or roles) with access to [*all security functions (examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions)*] use non-privileged accounts or roles, when accessing nonsecurity functions.

AC-6 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-6 (2) Describe how the control is implemented.	

13.1.17 AC-6 (5): Least Privilege | Privileged Accounts

Restrict privileged accounts on the system to [*GSA S/SO or Contractor recommended employees and contractors as approved by the GSA CISO and AO*].

AC-6 (5)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-6 (5) Describe how the control is implemented.	

AC-6 (5)	Control Enhancement Summary Information

13.1.18 AC-6 (7): Least Privilege | Review of User Privileges

(a) Review [*annually as part of the annual account review (per AC-2j)*] the privileges assigned to [*all roles and users*] to validate the need for such privileges; and
(b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

AC-6 (7)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-6 (7) Describe how the control is implemented.	
Part a	
Part b	

13.1.19 AC-6 (9): Least Privilege | Log Use of Privileged Functions

Log the execution of privileged functions.

AC-6 (9)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-6 (9) Describe how the control is implemented.	

13.1.20 AC-6 (10): Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions

Prevent non-privileged users from executing privileged functions.

AC-6 (10)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-6 (10) Describe how the control is implemented.	

AC-6 (10)	Control Enhancement Summary Information

13.1.21 AC-7: Unsuccessful Login Attempts

a. Enforce a limit of [*not more than ten (10) failed access attempts*] consecutive invalid logon attempts by a user during a [*30 minute time period*]; and
b. Automatically [*locks the account node for [30 minutes]*] when the maximum number of unsuccessful attempts is exceeded.

AC-7	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-7 Describe how the control is implemented.	
Part a	
Part b	

13.1.22 AC-8: System Use Notification

a. Display [*a system use notification message or banner as defined in GSA Order CIO 2100.1*] to users before granting access to the system that provides privacy and security notices

consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;

b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c. For publicly accessible systems:
   1. Displays system use information [*when accessed via logon interfaces with human users*], before granting further access;
   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Includes a description of the authorized uses of the system.

AC-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-8 Describe how the control is implemented.	
Part a	
Part b	

AC-8	Control Summary Information
Part c	

13.1.23 AC-11: Device Lock

a. Prevent further access to the system by [*initiating a device lock after 15 minutes of inactivity; requiring the user to initiate a device lock before leaving the system unattended*]; and

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

AC-11	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-11 Describe how the control is implemented.	
Part a	
Part b	

13.1.24 AC-11 (1): Device Lock | Pattern-Hiding Displays

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

AC-11 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-11 (1) Describe how the control is implemented.	

13.1.25 AC-12: Session Termination

Automatically terminate a user session after *[(1) 30 minutes of inactivity (2) the following timeframes, regardless of user activity: a. Thirty (30) days for systems at AAL1 b. Twelve (12) hours for systems at AAL2 and AAL3]. Note: AAL2 and AAL3 require Two Factor Authentication*].

AC-12	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-12 Describe how the control is implemented.	

AC-12	Control Summary Information

13.1.26 AC-14: Permitted Actions Without Identification or Authentication

a. Identify [*no user actions*] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and
b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

AC-14	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-14 Describe how the control is implemented.	
Part a	
Part b	

13.1.27 AC-17: Remote Access

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorizes remote access to the information system prior to allowing such connections.

AC-17	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-17 Describe how the control is implemented.	
Part a	
Part b	

13.1.28 AC-17 (1): Remote Access | Monitoring and Control

Employ automated mechanisms to monitor and control remote access methods.

AC-17 (1)	
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

AC-17 (1)	Control Enhancement Summary Information
AC-17(1) Describe how the control is implemented.	

13.1.29 AC-17 (2): Remote Access | Protection of Confidentiality and Integrity Using Encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AC-17 (2)	
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

13.1.30 AC-17 (3): Remote Access | Managed Access Control Points

Route remote accesses through authorized and managed network access control points.

AC-17 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

AC-17 (3)	Control Enhancement Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-17(3) Describe how the control is implemented.	

13.1.31 AC-17 (4): Remote Access | Privileged Commands/Access

(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [*S/SO or contractor recommended and GSA CISO and AO approved special cases for remote administration and maintenance tasks*]; and

(b) Document the rationale for remote access in the security plan for the system.

AC-17 (4)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-17 (4) Describe how the control is implemented.	

Part a	
Part b	

13.1.32 AC-18: Wireless Access

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and
b. Authorize each type of wireless access to the system prior to allowing such connections.

AC-18	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-18 Describe how the control is implemented.	
Part a	
Part b	

13.1.33 AC-18 (1): Wireless Access | Authentication and Encryption

Protect wireless access to the system using authentication of [*users and devices*] and encryption.

AC-18 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-18 (1) Describe how the control is implemented.	

13.1.34 AC-18 (3): Wireless Access | Disable Wireless Networking

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

AC-18 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

AC-18 (3)	Control Enhancement Summary Information
AC-18 (3) Describe how the control is implemented.	

13.1.35 AC-19: Access Control for Mobile Devices

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and
b. Authorize the connection of mobile devices to organizational systems.

AC-19	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: GSA Enterprise Application Services ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-19 Describe how the control is implemented.	
Part a	
Part b	

13.1.36 AC-19 (5): Access Control for Mobile Devices | Full Device or Container-Based Encryption

Employ [*at a minimum full device encryption, preferred container encryption*] to protect the

confidentiality and integrity of information on [*GSA approved and authorized mobile devices*].

AC-19 (5)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: GSA Enterprise Application Services ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-19 (5) Describe how the control is implemented.	

13.1.37 AC-20: Use of External Systems

a. [*Establish terms and conditions per agreements established by CA-3; and identify controls asserted to be implemented on external systems per agreements established by CA-3*], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
   1. Access the system from external systems; and
   2. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of [*external systems not covered by approved ISA, per CA-3*].

AC-20	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name]	

AC-20	Control Summary Information
☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-20 Describe how the control is implemented.	
Part a	
Part b	

13.1.38 AC-20 (1): Use of External Systems | Limits on Authorized Use

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

(a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or

(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

AC-20 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-20 (1) Describe how the control is implemented.	

AC-20 (1)	Control Enhancement Summary Information
Part a	
Part b	

13.1.39 AC-20 (2): Use of External Systems | Portable Storage Devices – Restricted Use

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [*prohibits the use of any external system that is not GSA owned including the use of personally-owned systems*].

AC-20 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: GSA Enterprise Application Services ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-20 (2) Describe how the control is implemented.	

13.1.40 AC-21: Information Sharing

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [*GSA S/SO or Contractor recommended information sharing circumstances where user discretion is required to be approved by the GSA CISO and AO*]; and

b. Employ [*GSA S/SO or Contractor recommended automated mechanisms or manual processes to be approved by the GSA CISO and AO*] to assist users in making information sharing and collaboration decisions.

AC-21	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-21 Describe how the control is implemented.	
Part a	
Part b	

13.1.41 AC-22: Publicly Accessible Content

a. Designate individuals authorized to make information publicly accessible;
b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and
d. Review the content on the publicly accessible system for nonpublic information [*quarterly*] and remove such information, if discovered.

AC-22	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented	

AC-22	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AC-22 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

13.2 Awareness and Training

13.2.1 AT-1: Policy and Procedures

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
   1. [*Organization-level*] awareness and training policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current awareness and training:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

AT-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Training and Awareness Program CIO-IT Security 05-29 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AT-1 Describe how the control is implemented.	
Part a	1. The GSA security awareness training policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding security awareness training for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Security awareness training procedures are documented in CIO-IT Security-05-29, "IT Security Procedural Guide: Security and Privacy Awareness and Role-Based Training Program." This guide is disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.

AT-1	Control Summary Information
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-05-29 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.2.2 AT-2: Literacy Training and Awareness

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
   1. As part of initial training for new users and [*annually*] thereafter; and
   2. When required by system changes or following [*the analysis of security trends, significant events, and user feedback*];
b. Employ the following techniques to increase the security and privacy awareness of system users [*by frequent phishing, security vignettes via email*];
c. Update literacy training and awareness content [*annually*] and following [*the analysis of security and privacy trends, significant events, and user feedback*]; and
d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

AT-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Configured by customer ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AT-2 Describe how the control is implemented.	

AT-2	Control Summary Information
Part a	
Part b	
Part c	
Part d	

13.2.3 AT-2 (2): Literacy Training and Awareness | Insider Threat

Provide literacy training on recognizing and reporting potential indicators of insider threat.

AT-2 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Configured by customer ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AT-2 (2) Describe how the control is implemented.	

AT-2 (2)	Control Enhancement Summary Information

13.2.4 AT-2 (3): Literacy Training and Awareness | Social Engineering and Mining

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

AT-2 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Configured by customer ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AT-2 (3) Describe how the control is implemented.	

13.2.5 AT-3: Role-Based Training

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [*CISO, AOs, System Owners, ISSMs, ISSOs, Privileged Users*]:
   1. Before authorizing access to the system, information, or performing assigned duties, and [*annually*] thereafter; and
   2. When required by system changes;
b. Update role-based training content [*annually*] and following [*the analysis of security and privacy trends, significant events, and user feedback*]; and
c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

AT-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AT-3 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.2.6 AT-3 (5): Role-Based Training | Processing Personally Identifiable Information

Provide [*all personnel with a GSA Account*] with initial and [*annual*] training in the employment and operation of personally identifiable information processing and transparency controls.

Note: Only applicable if PII is stored, processed, or transmitted by the system.

AT-3 (5)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation	

AT-3 (5)	Control Summary Information
☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AT-3 (5) Describe how the control is implemented.	

13.2.7 AT-4: Training Records

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and
b. Retains individual training records for [*three years*].

AT-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AT-4 Describe how the control is implemented.	
Part a	

AT-4	Control Summary Information
Part b	

13.3 Audit and Accountability

13.3.1 AU-1: Policy and Procedures

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

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

c. Review and update the current audit and accountability:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

AU-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Audit and Accountability (AU) CIO-IT Security-01-08 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

AU-1	Control Summary Information
AU-1 Describe how the control is implemented.	
Part a	1. The GSA audit and accountability policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding auditing and accountability for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Audit and accountability procedures are documented in CIO-IT Security-01-08, "IT Security Procedural Guide: Audit and Accountability (AU)." This guide is disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-01-08 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.3.2 AU-2: Event Logging

a. Identify the types of events that the system is capable of logging in support of the audit function: *[(1) successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events (2) Web applications should log all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes (3) for technologies with limited auditing features, the capabilities will be recommended by the GSA S/SO or Contractor, based on an industry source such as vendor guidance or Center for Internet Security benchmark, and approved by the GSA CISO and AO*];

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: [(*1) audit configuration requirements as documented in applicable GSA IT Security Technical Guides and Standards (i.e., hardening and technology implementation guides) (2) for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log (3) for technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor*

guidance or Center for Internet Security benchmark, recommended by the GSA S/SO or Contractor and approved by the GSA CISO and AO];

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [*annually or whenever there is a change in the system's threat environment as communicated by the GSA S/SO AO or the GSA OCISO*].

AU-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-2 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

AU-2	Control Summary Information
Part e	

13.3.3 AU-3: Content of Audit Records

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AU-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-3 Describe how the control is implemented.	
Part a	
Part b	

AU-3	Control Summary Information
Part c	
Part d	
Part e	
Part f	

13.3.4 AU-3 (1): Content of Audit Records | Additional Audit Information

Generates audit records containing the following additional information:[

i. Session, connection, transaction, or activity duration.

ii. For client-server transactions, the number of bytes received and bytes sent. This gives bidirectional transfer information that can be helpful during an investigation or inquiry.

iii. For client-server transactions, unique metadata or properties about the client initiating the transaction. This could include properties such as an IP address, user name, session identifier or browser characteristics (e.g. a 'User-Agent' string).

iv. Details regarding the event 'type': the type of method (for HTTP: GET/POST/HEAD, etc.) or action (Database INSERT, UPDATE, DELETE).

v. Characteristics that describe or identify the object or resource being acted upon.

vi. Additional informational messages to diagnose or identify the event].

AU-3 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination:	

AU-3 (1)	Control Enhancement Summary Information
☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-3 (1) Describe how the control is implemented.	

13.3.5 AU-3 (3): Content of Audit Records | Limit Personally Identifiable Information Elements

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [*no PII to be included in audit records*].

Note: Only applicable if PII is stored, processed, or transmitted by the system.

AU-3 (3)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-3 (3) Describe how the control is implemented.	

13.3.6 AU-4: Audit Storage Capacity

Allocate audit log storage capacity to accommodate [*GSA policies and guidance: audit log sizes are documented in applicable GSA IT Security Technical Guides and Standards (i.e., hardening and technology implementation guides) available on the IT Security Technical Guides and Standards webpage (https://insite.gsa.gov/topics/information-technology/security-and-privacy/it-security/it-security-technical-guides-and-standards)*].

AU-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-4 Describe how the control is implemented.	

13.3.7 AU-5: Response to Audit Processing Failures

a. Alert [*the GSA ISO Division via the Enterprise Logging Platform for systems integrated with it; Administrators (Application, System, Network, etc.) for systems not integrated with the Enterprise Logging Platform)*] within [*GSA S/SO or Contractor recommended time period as approved by the GSA CISO and AO*] in the event of an audit logging process failure; and

b. Take the following additional actions: [*shut down information system, overwrite oldest audit records, or stop generating audit records*].

AU-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

AU-5	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-5 Describe how the control is implemented.	
Part a	
Part b	

13.3.8 AU-6: Audit Record Review, Analysis, and Reporting

a. Review and analyze system audit records [*on business days when security related events are forwarded to the Enterprise Logging Platform for automated analysis and correlation, otherwise on a periodic basis (specific period recommended by the GSA S/SO or Contractor and approved by the GSA CISO and AO)*] for indications of [*GSA S/SO or Contractor recommended inappropriate or unusual activity as approved by the GSA CISO and AO*] and the potential impact of the inappropriate or unusual activity;

b. Report findings to [*Information System Security Manager, Information System Security Officer, System Owner, Custodian, as designated and approved by the GSA CISO and AO, via a dashboard when security related events are forwarded to the Enterprise Logging Platform, otherwise via manual reporting mechanisms*]; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

AU-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

AU-6	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-6 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.3.9 AU-6 (1): Audit Record Review, Analysis, and Reporting | Automated Process Integration

Integrate audit record review, analysis, and reporting processes using [*the GSA Enterprise Logging Platform for systems integrated with it; GSA S/SO or Contractor recommended automated mechanisms as approved by the GSA CISO and AO*].

AU-6 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control	

AU-6 (1)	Control Enhancement Summary Information
☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-6 (1) Describe how the control is implemented.	

13.3.10 AU-6 (3): Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

AU-6 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-6 (3) Describe how the control is implemented.	

13.3.11 AU-6 (4): Audit Record Review, Analysis, and Reporting | Central Review and Analysis

Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

AU-6 (4)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-6 (4) Describe how the control is implemented.	

13.3.12 AU-7: Audit Record Reduction and Report Generation

Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and

b. Does not alter the original content or time ordering of audit records.

AU-7	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-7 Describe how the control is implemented.	

AU-7	Control Summary Information
Part a	
Part b	

13.3.13 AU-7 (1): Audit Record Reduction and Report Generation | Automatic Processing

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [*Source IP, Destination IP, Account Names, Date and Time of Events, Event Type*].

AU-7 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-7 (1) Describe how the control is implemented.	

13.3.14 AU-8: Time Stamps

a. Use internal system clocks to generate time stamps for audit records; and
b. Record time stamps for audit records that meet [*GSA S/SO or Contractor recommended granularity of time measurement to be approved by the GSA CISO and AO*] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

AU-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-8 Describe how the control is implemented.	
Part a	
Part b	

13.3.15 AU-9: Protection of Audit Information

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and
b. Alert [*the GSA Incident Response Team*] upon detection of unauthorized access, modification, or deletion of audit information.

AU-9	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control	

AU-9	Control Summary Information
☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-9 Describe how the control is implemented.	
Part a	
Part b	

13.3.16 AU-9 (4): Protection of Audit Information | Access by Subset of Privileged Users

Authorize access to management of audit logging functionality to only [*privileged users specifically authorized to perform audit management functions (i.e., specified administrators of applications, systems, networks, etc.)*].

AU-9 (4)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-9 (4) Describe how the control is implemented.	

13.3.17 AU-11: Audit Record Retention

Retain audit records for [*archived for a period of not less than 180 days*] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AU-11	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-11 Describe how the control is implemented.	

13.3.18 AU-12: Audit Generation

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [*all components*];
b. Allow [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*] to select the event types that are to be logged by specific components of the system; and
c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

AU-12	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation	

AU-12	Control Summary Information
☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
AU-12 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.4 Assessment, Authorization, and Monitoring

13.4.1 CA-1: Policy and Procedures

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

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

c. Review and update the current assessment, authorization, and monitoring:

1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

CA-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk Security Assessment and Authorization, Planning, and Risk Assessment (CA, PL, & RA) CIO-IT Security-06-30. ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CA-1 Describe how the control is implemented.	
Part a	1. The GSA security assessment and authorization policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding assessing and authorizing systems for GSA. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Security assessment and authorization procedures are documented in CIO-IT Security-06-30, "IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk." Additional security and assessment guides for specific types of systems have been developed and are referenced in CIO-IT Security-06-30. The procedures in these guides facilitate the security assessment and authorization of all GSA systems. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.

CA-1	Control Summary Information
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-06-30 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.4.2 CA-2: Control Assessments

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

CA-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CA-2 Describe how the control is implemented.	

CA-2	Control Summary Information
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	

13.4.3 CA-2 (1): Control Assessments | Independent Assessors

Employ independent assessors or assessment teams to conduct control assessments.

Note: Assessors are independent if they do not: (i) have a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are assessing; or (iv) place themselves in positions of advocacy for the organizations acquiring their services.

CA-2 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation	

CA-2 (1)	Control Enhancement Summary Information
☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CA-2 (1) Describe how the control is implemented.	

13.4.4 CA-3: Information Exchange

a. Approve and manage the exchange of information between the system and other systems using [*interconnection security agreements as applicable per 06-30 and documented in the system's SSPP interconnection section (Table 11-1 and 11-2)*]
b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
c. Review and update the agreements [*at least annually*].

CA-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CA-3 Describe how the control is implemented.	

CA-3	Control Summary Information
Part a	
Part b	
Part c	

13.4.5 CA-5: Plan of Action and Milestones

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

CA-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CA-5 Describe how the control is implemented.	

CA-5	Control Summary Information
Part a	
Part b	

13.4.6 CA-6: Authorization

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

CA-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CA-6 Describe how the control is implemented.	

CA-6	Control Summary Information
Part a	
Part b	
Part c	
Part d	
Part e	

13.4.7 CA-7: Continuous Monitoring

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

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

g. Reporting the security and privacy status of the system to [*CISO, AOs, System Owners, ISSMs, ISSOs, Custodians] [as specified in in Section 3 of CIO-IT Security-08-39, Management Implementation Plan and CIO-IT Security-12-66, ISCM Strategy and OA Program*].

CA-7	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CA-7 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	

CA-7	Control Summary Information
Part f	
Part g	

13.4.8 CA-7 (1): Continuous Monitoring | Independent Assessment

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.
Note: Independence is waived for all annual testing (i.e., testing can be internally performed).

CA-7 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CA-7 (1) Describe how the control is implemented.	

13.4.9 CA-7 (4): Continuous Monitoring | Risk Monitoring

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:
(a) Effectiveness monitoring;
(b) Compliance monitoring; and

(c) Change monitoring.

CA-7 (4)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CA-7 (4) Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.4.10 CA-8: Penetration Testing

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

CA-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

CA-8	Control Summary Information
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CA-8 Describe how the control is implemented.	

13.4.11 CA-8 (1): Penetration Testing | Independent Penetration Testing Agent or Team

Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

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

CA-8 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CA-8 (1) Describe how the control is implemented.	

13.4.12 CA-9: Internal System Connections

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

CA-9	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CA-9 Describe how the control is implemented.	
Part a	
Part b	
Part c	

CA-9	Control Summary Information
Part d	

13.5 Configuration Management

13.5.1 CM-1: Policy and Procedures

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

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and

c. Review and update the current configuration management:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

CM-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, IT Security Procedural Guide: Configuration Management (CM) CIO-IT Security-01-05 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

CM-1	Control Summary Information
CM-1 Describe how the control is implemented.	
Part a	1. The GSA configuration management policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding configuration management of GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Configuration management procedures are documented in CIO-IT Security-01-05, "IT Security Procedural Guide: Configuration Management (CM)." The procedures facilitate the implementation of the configuration management policy and associated controls. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-01-05 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.5.2 CM-2: Baseline Configuration

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:

1. [*Annually*];
2. When required due to [*significant change as defined in NIST SP 800-37 Revision 2, Appendix F*]; and
3. When system components are installed or upgraded.

CM-2	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

CM-2	Control Enhancement Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-2 Describe how the control is implemented.	
Part a	
Part b	

13.5.3 CM-2 (2): Baseline Configuration | Automation Support for Accuracy and Currency

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [*automated mechanisms as identified in the SSPP/CM Plan*].

CM-2 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-2 (2) Describe how the control is implemented.	

CM-2 (2)	Control Enhancement Summary Information

13.5.4 CM-2 (3): Baseline Configuration | Retention of Previous Configurations

Retain [*GSA S/SO or Contractor recommended number of previous versions of baseline configurations of the system approved by the GSA CISO and AO*] of previous versions of baseline configurations of the system to support rollback.

CM-2 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-2 (3) Describe how the control is implemented.	

13.5.5 CM-2 (7): Baseline Configuration | Configure Systems and Components for High-Risk Areas

(a) Issue [*specially configured notebook computers with sanitized hard drives*] with [*limited applications, and additional hardening (e.g., more stringent configuration settings)*] to individuals traveling to locations that the organization deems to be of significant risk; and
(b) Apply the following controls to the systems or components when the individuals return from travel: [*GSA standards (e.g., baseline configuration, system image, standard build configuration). Reference the GSA Enterprise Architecture Committee (EARC) Approved IT Standards at - https://ea.gsa.gov/#!/itstandards*].

CM-2 (7)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-2 (7) Describe how the control is implemented.	
Part a	
Part b	

13.5.6 CM-3: Configuration Change Control

a. Determine and document the types of changes to the system that are configuration-controlled;
b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
c. Document configuration change decisions associated with the system;
d. Implement approved configuration-controlled changes to the system;
e. Retain records of configuration-controlled changes to the system forr [*as long as deemed necessary by GSA S/SO or Contractor and approved by the GSA CISO and AO*];
f. Monitor and review activities associated with configuration-controlled changes to the system; and
g. Coordinate and provide oversight for configuration change control activities through [*a defined CM approval process (example: a charted Configuration Change Board (CCB))*]; that convenes [*on a defined basis in support of the system's CM requirements*]; [*to approve changes such as:*
   - *Upgrades and modifications to the information system or its components*

- *Changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers)*
- *Emergency changes required to address an immediate issue*
- *Changes to remediate flaws*].

CM-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-3 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	

CM-3	Control Summary Information
Part f	
Part g	

13.5.7 CM-3 (1): Configuration Change Control | Automated Document, Notification, and Prohibition of Changes

Use [*automated mechanisms as identified in the SSPP/CM Plan*] to:

(a) Document proposed changes to the system;

(b) Notify [*GSA S/SO or Contractor recommended approval authorities approved by the GSA CISO and AO*] of proposed changes to the system and request change approval;

(c) Highlight proposed changes to the system that have not been approved or disapproved within [*GSA S/SO or Contractor recommended time period approved by the GSA CISO and AO*];

(d) Prohibit changes to the system until designated approvals are received;

(e) Document all changes to the system; and

(f) Notify [*Administrators (Application, System, Network, etc.), Information System Security Officer, Information System Security Manager, System Owner (e.g., System Program Manager, System Project Manager)*] when approved changes to the system are completed.

CM-3 (1)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-3 (1) Describe how the control is implemented.	

CM-3 (1)	Control Summary Information
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	

13.5.8 CM-3 (2): Configuration Change Control | Testing, Validation, and Documentation of Changes

Test, validate, and document changes to the system before finalizing the implementation of the changes.

CM-3 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination:	

CM-3 (2)	Control Enhancement Summary Information
☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-3 (2) Describe how the control is implemented.	

13.5.9 CM-3 (4): Configuration Change Control | Security and Privacy Representatives

Require [*security and privacy representatives as defined in the SSPP/CM Plan*] to be members of the [*defined configuration change control element (e.g., a charted Configuration Change Board (CCB))*].

CM-3 (4)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-3 (4) Describe how the control is implemented.	

13.5.10 CM-4: Impact Analyses

Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

CM-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-4 Describe how the control is implemented.	

13.5.11 CM-4 (2): Impact Analyses | Verification of Controls

After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

CM-4 (2)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-4 (2) Describe how the control is implemented.	

CM-4 (2)	Control Summary Information

13.5.12 CM-5: Access Restrictions for Change

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

CM-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Configured by customer ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-5 Describe how the control is implemented.	

13.5.13 CM-6: Configuration Settings

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [*GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as reviewed and accepted by the GSA CISO and AO*];
b. Implement the configuration settings;
c. Identify, document, and approve any deviations from established configuration settings for [*all components*] based on [*explicit operational requirements*]; and
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

CM-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-6 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

13.5.14 CM-6 (1): Configuration Settings | Automated Management Application, and Verification

Manage, apply, and verify configuration settings for [*all operating systems*] using [*automated mechanisms as documented in the SSPP/CM Plan*].

CM-6 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented	

CM-6 (1)	Control Enhancement Summary Information
☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Configured by customer ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-6 (1) Describe how the control is implemented.	

13.5.15 CM-7: Least Functionality

a. Configure the system to provide only [*mission essential capabilities in accordance with the Business Impact Analysis (BIA)*]; and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [*as specified in GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as deemed appropriate by the GSA CISO and AO*].

CM-7	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

CM-7	Control Summary Information
CM-7 Describe how the control is implemented.	
Part a	
Part b	

13.5.16 CM-7 (1): Least Functionality | Periodic Review

(a) Review the system [*annually as part of SSPP update*] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

(b) Disable or remove [*GSA S/SO or Contractor recommended functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure as approved by the GSA CISO and AO*].

CM-7 (1)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Configured by customer ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-7 (1) Describe how the control is implemented.	
Part a	

CM-7 (1)	Control Summary Information
Part b	

13.5.17 CM-7 (2): Least Functionality | Prevent Program Execution

Prevent program execution in accordance with [*CIO 2100.1 policies and GSA S/SO or Contractor recommended list of authorized software programs, a list of unauthorized software programs, and rules authorizing the terms and conditions of software program usage, as approved by the GSA CISO and AO*].

CM-7 (2)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Configured by customer ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-7 (2) Describe how the control is implemented.	

13.5.18 CM-7 (5): Least Functionality | Authorized Software – Allow-By-Exception

(a) Identify [*GSA S/SO or Contractor recommended software programs authorized to execute on the information system as approved by the GSA CISO and AO*];
(b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and
(c) Review and update the list of authorized software programs [*annually as part of SSPP update*].

CM-7 (5)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Configured by customer ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-7 (5) Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.5.19 CM-8: System Component Inventory

a. Develop and document an inventory of information system components that:
   1. Accurately reflects the system;
   2. Includes all components within the system;
   3. Does not include duplicate accounting of components or components assigned to any other system;
   4. Is at the level of granularity deemed necessary for tracking and reporting; and
   5. Includes the following information to achieve system component accountability: [*GSA S/SO or Contractor recommended information deemed necessary to ensure property accountability as approved by the GSA CISO and AO. List may include hardware inventory specifications (manufacturer, type, model, serial number, physical location), software*

license information, information system/component owner, and for a networked component/device, the machine name and network address]; and

b. Review and update the system component inventory [*monthly*].

CM-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-8 Describe how the control is implemented.	
Part a	
Part b	

13.5.20 CM-8 (1): System Component Inventory | Updates During Installations and Removals

Update the inventory of system components as part of component installations, removals, and system updates.

CM-8 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

CM-8 (1)	Control Enhancement Summary Information
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-8 (1) Describe how the control is implemented.	

13.5.21 CM-8 (2): System Component Inventory | Automated Maintenance

Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [*automated mechanisms as documented in the SSPP/CM Plan*].

CM-8 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-8 (2) Describe how the control is implemented.	

13.5.22 CM-8 (3): System Component Inventory | Automated Unauthorized Component Detection

(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [*automated mechanisms as defined in the SSPP/CM Plan*] [*on an ongoing basis*]; and

(b) Take the following actions when unauthorized components are detected: [*isolates the components and notifies GSA S/SO or Contractor recommended and GSA approved personnel or roles*].

CM-8 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-8 (3) Describe how the control is implemented.	
Part a	
Part b	

13.5.23 CM-8 (6): Information System Component Inventory | Assessed Configurations and Approved Deviations

Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.

CM-8 (6)	Control Enhancement Summary Information
Implementation Status:	

CM-8 (6)	Control Enhancement Summary Information
☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-8 (6) Describe how the control is implemented.	

13.5.24 CM-8 (7): System Component Inventory | Centralized Repository

Provide a centralized repository for the inventory of system components.

CM-8 (7)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-8 (7) Describe how the control is implemented.	

13.5.25 CM-9: Configuration Management Plan

Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the system and places the configuration items under configuration management;
d. Is reviewed and approved by [*defined CM personnel (e.g., charted Configuration Change Board (CCB))*]; and
e. Protects the configuration management plan from unauthorized disclosure and modification.

CM-9	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-9 Describe how the control is implemented.	
Part a	
Part b	
Part c	

CM-9	Control Summary Information
Part d	
Part e	

13.5.26 CM-10: Software Usage Restrictions

a. Use software and associated documentation in accordance with contract agreements and copyright laws;
b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

CM-10	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-10 Describe how the control is implemented.	
Part a	

CM-10	Control Summary Information
Part b	
Part c	

13.5.27 CM-11: User-Installed Software

a. Establish [*policies as specified in CIO 2100.1*] governing the installation of software by users;
b. Enforce software installation policies through the following methods: [*automated methods (i.e., configuration/compliance scans)*]; and
c. Monitor policy compliance [*on an ongoing basis*].

CM-11	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-11 Describe how the control is implemented.	
Part a	
Part b	

CM-11	Control Summary Information
Part c	

13.5.28 CM-12: Information Location

a. Identify and document the location of [*Personally Identifiable Information (PII); Payment Card Industry (PCI) data; Identity, Credentialing, and Access Management (ICAM) data (includes but is not limited to identifier and authenticator data such as passwords, tokens, keys, certificates, hashes); system- and application-security log data; and, other sensitive data as determined by the GSA CISO and AO*] and the specific system components on which the information is processed and stored;
b. Identify and document the users who have access to the system and system components where the information is processed and stored; and
c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

CM-12	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-12 Describe how the control is implemented.	
Part a	

CM-12	Control Summary Information
Part b	
Part c	

13.5.29 CM-12 (1): Information Location | Automated Tools to Support Information Location

Use automated tools to identify [*Personally Identifiable Information (PII); Payment Card Industry (PCI) data; Identity, Credentialing, and Access Management (ICAM) data (includes but is not limited to identifier and authenticator data such as passwords, tokens, keys, certificates, hashes); system- and application-security log data; and, other sensitive data as determined by the GSA CISO and AO*] on [*all system components for external information systems*] to ensure controls are in place to protect organizational information and individual privacy.

CM-12 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CM-12 (1) Describe how the control is implemented.	

13.6 Contingency Planning

13.6.1 CP-1: Policy and Procedures

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

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

CP-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Contingency Planning (CP) CIO-IT Security-06-29 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-1 Describe how the control is implemented.	
Part a	1. The GSA contingency planning policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding the contingency planning for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies,

CP-1	Control Summary Information
	standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Contingency planning procedures are documented in CIO-IT Security-06-29, "IT Security Procedural Guide: Contingency Planning (CP)." The procedures facilitate the implementation of the contingency planning policy and associated controls. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-06-29 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.6.2 CP-2: Contingency Plan

a. Develop a contingency plan for the system that:
   1. Identifies essential mission and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
   5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
   6. Addresses the sharing of contingency information; and
   7. Is reviewed and approved by [the Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), Program Manager (PM), Chief Information Security Officer (CISO), and the Emergency Response Coordinator (ERC)];

b. Distribute copies of the contingency plan to [*the Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), Program Manager (PM), Office of the Chief Information Security Officer (CISO), and the Emergency Response Coordinator (ERC)*];

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system [*annually*];
e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicate contingency plan changes to [*Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), Program Manager (PM), Chief Information Security Officer (CISO), and Emergency Response Coordinator (ERC)*];
g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
h. Protect the contingency plan from unauthorized disclosure and modification.

CP-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-2 Describe how the control is implemented.	
Part a	
Part b	
Part c	

CP-2	Control Summary Information
Part d	
Part e	
Part f	
Part g	
Part h	

13.6.3 CP-2 (1): Contingency Plan | Coordinate With Related Plans

Coordinate contingency plan development with organizational elements responsible for related plans.

CP-2 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

CP-2 (1)	Control Enhancement Summary Information
CP-2 (1) Describe how the control is implemented.	

13.6.4 CP-2 (3): Contingency Plan | Resume Mission and Business Functions

Plan for the resumption of [*all*] mission and business functions within [*a time period recommended by the GSA S/SO or Contractor in accordance with the Business Impact Analysis (BIA) and approved by the GSA CISO and AO*] of contingency plan activation.

CP-2 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-2 (3) Describe how the control is implemented.	

13.6.5 CP-2 (8): Contingency Plan | Identify Critical Assets

Identify critical system assets supporting [*all*] mission and business functions.

CP-2 (8)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

CP-2 (8)	Control Enhancement Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-2 (8) Describe how the control is implemented.	

13.6.6 CP-3: Contingency Training

a. Provide contingency training to system users consistent with assigned roles and responsibilities:
   1. Within [*30 days*] of assuming a contingency role or responsibility;
   2. When required by system changes; and
   3. [*Every two years*] thereafter; and

b. Review and update contingency training content [*every two years*] and following [*incidents that impacted continuity of operations*].

CP-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-3 Describe how the control is implemented.	

CP-3	Control Summary Information
Part a	
Part b	

13.6.7 CP-4: Contingency Plan Testing

a. Test the contingency plan for the information system [*annually*] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [*GSA IT Security Procedural Guide: Contingency Planning (CP) CIO-IT Security-06-29*].
b. Reviews the contingency plan test results; and
c. Initiate corrective actions, if needed.

CP-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-4 Describe how the control is implemented.	
Part a	
Part b	

CP-4	Control Summary Information
Part c	

13.6.8 CP-4 (1): Contingency Plan Testing | Coordinate With Related Plans

Coordinate contingency plan testing with organizational elements responsible for related plans.

CP-4 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-4 (1) Describe how the control is implemented.	

13.6.9 CP-6: Alternate Storage Site

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and
b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

CP-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

CP-6	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-6 Describe how the control is implemented.	
Part a	
Part b	

13.6.10 CP-6 (1): Alternate Storage Site | Separation from Primary Site

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

CP-6 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

CP-6 (1)	Control Enhancement Summary Information
CP-6 (1) Describe how the control is implemented.	

13.6.11 CP-6 (3): Alternate Storage Site | Accessibility

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

CP-6 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-6 (3) Describe how the control is implemented.	

13.6.12 CP-7: Alternate Processing Site

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [*information system operations*] for essential mission and business functions within [*GSA S/SO or Contractor recommended time period approved by the GSA CISO and AO consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable;
b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

CP-7	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-7 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.6.13 CP-7 (1): Alternate Processing Site | Separation from Primary Site

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

CP-7 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

CP-7 (1)	Control Enhancement Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-7 (1) Describe how the control is implemented.	

13.6.14 CP-7 (2): Alternate Processing Site | Accessibility

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-7 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-7 (2) Describe how the control is implemented.	

13.6.15 CP-7 (3): Alternate Processing Site | Priority of Service

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

CP-7 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-7 (3) Describe how the control is implemented.	

13.6.16 CP-8: Telecommunications Services

Establish alternate telecommunications services, including necessary agreements to permit the resumption of [*information system operations*] for essential mission and business functions within [*GSA S/SO or Contractor recommended time period approved by the GSA CISO and AO*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name]	

CP-8	Control Summary Information
☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-8 Describe how the control is implemented.	

13.6.17 CP-8 (1): Telecommunications Services | Priority of Service Provisions

(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and

(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

CP-8 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-8 (1) Describe how the control is implemented.	
Part a	

CP-8 (1)	Control Enhancement Summary Information
Part b	

13.6.18 CP-8 (2): Telecommunications Services | Single Points of Failure

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

CP-8 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-8 (2) Describe how the control is implemented.	

13.6.19 CP-9: System Backup

a. Conduct backups of user-level information contained in [*non-user issued components (e.g., laptops, desktops*] [*in the BIA such that backup frequency supports the system's recovery time and recovery point objectives*];
b. Conduct backups of system-level information contained in the system [*BIA such that backup frequency supports the system's recovery time and recovery point objectives*];
c. Conduct backups of system documentation, including security- and privacy-related documentation [*BIA such that backup frequency supports the system's recovery time and recovery point objectives*]; and
d. Protect the confidentiality, integrity, and availability of backup information.

CP-9	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-9 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

13.6.20 CP-9 (1): System Backup | Testing for Reliability and Integrity

Test backup information [*at least annually*] to verify media reliability and information integrity.

CP-9 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

CP-9 (1)	Control Enhancement Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-9 (1) Describe how the control is implemented.	

13.6.21 CP-9 (8): System Backup | Cryptographic Protection

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [*all backup data*].

CP-9 (8)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-9 (5) Describe how the control is implemented.	

13.6.22 CP-10: System Recovery and Reconstitution

Provide for the recovery and reconstitution of the system to a known state within [*the defined time period, documented by the CP Plan and approved by the GSA CISO and AO, such that the system's recovery time and recovery point objectives are met*] after a disruption, compromise, or failure.

CP-10	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
CP-10 Describe how the control is implemented.	

13.6.23 CP-10 (2): System Recovery and Reconstitution | Transaction Recovery

Implement transaction recovery for systems that are transaction-based.

CP-10 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's	

CP-10 (2)	Control Enhancement Summary Information
Name] SSPP) ☐ System Specific Control	
CP-10 (2) Describe how the control is implemented.	

13.7 Identification and Authentication

13.7.1 IA-1: Policy and Procedures

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

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

IA-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Identification and Authentication (IA) CIO-IT Security-01-01	

IA-1	Control Summary Information
☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-1 Describe how the control is implemented.	
Part a	1. The GSA identification and authentication policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding the identification and authentication for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Identification and authentication procedures are documented in CIO-IT Security-01-01, "IT Security Procedural Guide: Identification and Authentication (IA)." The procedures facilitate the implementation of the identification and authentication policy and associated controls. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-01-01 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.7.2 IA-2: Identification and Authentication (Organizational Users)

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

IA-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation	

☐ Not applicable
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control
IA-2 Describe how the control is implemented.

13.7.3 IA-2 (1): Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts

Implement multi-factor authentication for access to privileged accounts.

IA-2 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-2 (1) Describe how the control is implemented.	

13.7.4 IA-2 (2): Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts

Implement multi-factor authentication for access to non-privileged accounts.

IA-2 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-2 (2) Describe how the control is implemented.	

13.7.5 IA-2 (8): Identification and Authentication (Organizational Users) |Access to Accounts – Replay Resistant

Implement replay-resistant authentication mechanisms for access to [*privileged and non-privileged accounts*].

IA-2 (8)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's	

IA-2 (8)	Control Enhancement Summary Information
Name] SSPP) ☐ System Specific Control	
IA-2 (8) Describe how the control is implemented.	

13.7.6 IA-2 (12): Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials

Accept and electronically verify Personal Identity Verification-compliant credentials.

IA-2 (12)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-2 (12) Describe how the control is implemented.	

13.7.7 IA-3: Device Identification and Authentication

Uniquely identify and authenticate [*GSA S/SO or Contractor recommended and GSA CISO and AO approved specific and/or types of devices*] before establishing a [*local, remote, or network*] connection.

IA-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-3 Describe how the control is implemented.	

13.7.8 IA-4: Identifier Management

Manage system identifiers by:

a. Receiving authorization from [*personnel with identifier assignment authorization as defined in GSA CIO Order 2100.1*] to assign an individual, group, role, service, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, service, or device;
c. Assigning the identifier to the intended individual, group, role, service, or device; and
d. Preventing reuse of identifiers for [*GSA S/SO or Contractor recommended and AO approved time period*].

IA-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's	

IA-4	Control Summary Information
Name] SSPP) ☐ System Specific Control	
IA-4 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

13.7.9 IA-4 (4): Identifier Management | Identify User Status

Manage individual identifiers by uniquely identifying each individual as [*GSA S/SO or Contractor recommended characteristic to be approved by the GSA CISO and AO*].

IA-4 (4)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

IA-4 (4)	Control Summary Information
IA-4 (4) Describe how the control is implemented.	

13.7.10 IA-5: Authenticator Management

Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
b. Establishing initial authenticator content for any authenticators issued by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
e. Changing default authenticators prior to first use;
f. Changing or refreshing authenticators [*every 90 days for single factor authenticators (e.g., passwords); only upon reissuance for multi-factor authenticators; one time use passwords must expire in: (1) two minutes if based on a real-time clock, (2) ten minutes if sent by means other than physical mail, (3) seven days if sent to a postal address of record, (4) twenty-one days if an exception is granted to accommodate an address of record outside the direct reach of the U.S. Postal Service*] or when [*compromised, recovered/forgotten, or due to incident related events*] occur;
g. Protecting authenticator content from unauthorized disclosure and modification;
h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
i. Changing authenticators for group or role accounts when membership to those accounts changes.

IA-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name]	

IA-5	Control Summary Information
☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-5 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	

IA-5	Control Summary Information
Part i	

13.7.11 IA-5 (1): Authenticator Management | Password-Based Authentication

For password-based authentication:

(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [*within 12 months of the latest available version of the utilized bad password database checking service (e.g., haveibeenpwned.com)*] and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;
(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery;
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules: [*Systems using a NIST SP 800-63B compliant password checking solution, passwords SHALL be at least 8 characters in length if chosen by the user; passwords chosen randomly by the system SHALL be at least 6 characters in length and MAY be entirely numeric. No other complexity requirements are required. See NIST SP 800-63B Memorized Secret (Section 5.1.1) for additional guidance.*

Systems NOT using a NIST 800-63B compliant passworing checking solution, SHALL use the following composition and complexity rules:

(1) Passwords for accounts used to access operating systems (workstations and servers) must contain a minimum of sixteen (16) characters with no complexity requirement.

(2) Passwords for systems/other accounts (e.g., service, application) must contain a minimum of eight (8) characters, and require a combination of letters, numbers, and special characters
(3) Passwords for all mobile devices such as GSA approved smart phones, iPads, and tablets must be a minimum of 6 characters. The six-character password requirement also applies to personal mobile devices accessing GSA data or systems.].

IA-5 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-5 (1) Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	

IA-5 (1)	Control Enhancement Summary Information
Part g	
Part h	

13.7.12 IA-5 (2): Authenticator Management | Public Key-Based Authentication

(a) For public key-based authentication:
  (1) Enforce authorized access to the corresponding private key; and
  (2) Map the authenticated identity to the account of the individual or group; and
(b) When public key infrastructure (PKI) is used:
  (1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
  (2) Implement a local cache of revocation data to support path discovery and validation.

IA-5 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-5 (2) Describe how the control is implemented.	
Part a	

IA-5 (2)	Control Enhancement Summary Information
Part b	

13.7.13 IA-5 (6): Authenticator Management | Protection of Authenticators

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

IA-5 (6)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-5 (6) Describe how the control is implemented.	

13.7.14 IA-5 (7): Authenticator Management | No Embedded Unencrypted Static Authenticators

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

IA-5 (7)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

IA-5 (7)	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-5 (7) Describe how the control is implemented.	

13.7.15 IA-6: Authenticator Feedback

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

IA-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-6 Describe how the control is implemented.	

13.7.16 IA-7: Cryptographic Module Authentication

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

IA-7	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-7 Describe how the control is implemented.	

13.7.17 IA-8: Identification and Authentication (Non-Organizational Users)

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

IA-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's	

IA-8	Control Summary Information
Name] SSPP) ☐ System Specific Control	
IA-8 Describe how the control is implemented.	

13.7.18 IA-8 (1): Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

IA-8 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-8 (1) Describe how the control is implemented.	

13.7.19 IA-8 (2): Identification and Authentication (Non-Organizational Users) | Acceptance of External Party Credentials

(a) Accept only external authenticators that are NIST-compliant; and
(b) Document and maintain a list of accepted external authenticators.

IA-8 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-8 (2) Describe how the control is implemented.	
Part a	
Part b	

13.7.20 IA-8 (4): Identification and Authentication (Non-Organizational Users) | Use of Defined Profiles

Conform to the following profiles for identity management [per each system's defined external user roles (See SSPP Section: Types of Users)].

IA-8 (4)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's	

IA-8 (4)	Control Enhancement Summary Information
Name] SSPP) ☐ System Specific Control	
IA-8 (4) Describe how the control is implemented.	

13.7.21 IA-11: Re-Authentication

Require users to re-authenticate when [*Passwords are reset, privileged functions are executed, and/or periodic reauthentication time limits are met. Reauthentication times are predicated on NIST 800-63B Authenticator Assurance Levels (See Section 4). Specifically:*
(1) After 30 minutes of inactivity at all levels;
(2) The following timeframes regardless of user activity
a. Thirty (30) days for systems at AAL1;
b. Twelve (12) hours for systems at AAL2 and AAL3].

Note: AAL3 requires presentation of all authentication factors, AAL2 (although requiring MFA) and AAL1 allow a single factor to be presented for re-authentication.

IA-11	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-11 Describe how the control is implemented.	

13.7.22 IA-12: Identity Proofing

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;
b. Resolve user identities to a unique individual; and
c. Collect, validate, and verify identity evidence.

IA-12	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-12 Describe how the control is implemented.	

13.7.23 IA-12 (2): Identity Proofing | Identity Evidence

Require evidence of individual identification be presented to the registration authority.

IA-12 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's	

IA-12 (2)	Control Enhancement Summary Information
Name] SSPP) ☐ System Specific Control	
IA-12 (2) Describe how the control is implemented.	

13.7.24 IA-12 (3): Identity Proofing | Identity Evidence Validation and Verification

Require that the presented identity evidence be validated and verified through [*mechanism(s) that support the IAL level determined when completing the GSA digital identity acceptance statement*].

Note: Control implementation details must describe the mechanisms used and how they meet the IAL level requirements.

IA-12 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-12 (3) Describe how the control is implemented.	

13.7.25 IA-12 (5): Identity Proofing | Address Confirmation

Require that a [*notice of proofing (applicable to IAL2 and IAL3 systems) in accordance with NIST SP 800-63A, and the GSA digital identity acceptance statement for the application*] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

IA-12 (5)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IA-12 (5) Describe how the control is implemented.	

13.8 Incident Response

13.8.1 IR-1: Policy and Procedures

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

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

IR-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Incident Response (IR) CIO-IT Security-01-02 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-1 Describe how the control is implemented.	
Part a	1. The GSA incident response policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding the incident response for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Incident response procedures are documented in CIO-IT Security-01-02, "IT Security Procedural Guide: Incident Response (IR)." The procedures facilitate the implementation of the incident response policy and associated controls. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-01-02 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.8.2 IR-2: Incident Response Training

a. Provide incident response training to system users consistent with assigned roles and responsibilities:
   1. Within [*60 days*] of assuming an incident response role or responsibility or acquiring system access;
   2. When required by system changes; and
   3. [*annually*] thereafter; and

b. Review and update incident response training content [*annually*] and following [*significant incidents as determined by the GSA Incident Response team*].

IR-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-2 Describe how the control is implemented.	
Part a	
Part b	

13.8.3 IR-2 (3): Incident Response Training | Breach

Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

Note: Only applicable if PII is stored, processed, or transmitted by the system.

IR-2 (3)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-2 (3) Describe how the control is implemented.	

13.8.4 IR-3: Incident Response Testing

Test the effectiveness of the incident response capability for the system [*annually*] using the following tests: [*as described in GSA IT Security Procedural Guide: Incident Response (IR) CIO- IT Security-01-02 and NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide*].

IR-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

IR-3	Control Summary Information
IR-3 Describe how the control is implemented.	

13.8.5 IR-3 (2): Incident Response Testing | Coordination with Related Plans

Coordinate incident response testing with organizational elements responsible for related plans.

IR-3 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-3 (2) Describe how the control is implemented.	

13.8.6 IR-4: Incident Handling

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinate incident handling activities with contingency planning activities;
c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and
d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

IR-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-4 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.8.7 IR-4 (1): Incident Handling | Automated Incident Handling Processes

Support the incident handling process using [*Federal: GSA IT Service Now; Contractor: GSA S/SO or Contractor recommended and AO approved automated mechanisms*].

IR-4 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

IR-4 (1)	Control Enhancement Summary Information
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-4 (1) Describe how the control is implemented.	

13.8.8 IR-5: Incident Monitoring

Track and document incidents.

IR-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-5 Describe how the control is implemented.	

13.8.9 IR-6: Incident Reporting

a. Require personnel to report suspected incidents to the organizational incident response capability within [*US-CERT Incident Reporting Timelines as documented in GSA IT Security Procedural Guide : Incident Response (IR) CIO- IT Security-01-02*]; and

b. Report incident information to [*the ISSO and Help Desk as per GSA IT Security Procedural Guide: Incident Response (IR) CIO- IT Security-01-02. Incidents classified between Categories 1-3 should simultaneously be reported to the OCISO*].

IR-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-6 Describe how the control is implemented.	
Part a	
Part b	

13.8.10 IR-6 (1): Incident Reporting | Automated Reporting

Report incidents using [*Federal: GSA IT Service Now; Contractor: GSA S/SO or Contractor recommended and GSA CISO and AO approved automated mechanisms*].

IR-6 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination:	

IR-6 (1)	Control Enhancement Summary Information
☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-6 (1) Describe how the control is implemented.	

13.8.11 IR-6 (3): Incident Reporting | Supply Chain Coordination

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

IR-6 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-6 (3) Describe how the control is implemented.	

13.8.12 IR-7: Incident Response Assistance

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

IR-7	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-7 Describe how the control is implemented.	

13.8.13 IR-7 (1): Incident Response Assistance | Automation Support for Availability of Information and Support

Increase the availability of incident response information and support using [*Federal: GSA IT Service Now; Contractor: GSA S/SO or Contractor recommended and GSA CISO and AO approved automated mechanisms*].

IR-7 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name]	

IR-7 (1)	Control Enhancement Summary Information
☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-7 (1) Describe how the control is implemented.	

13.8.14 IR-8: Incident Response Plan

a. Develop an incident response plan that:
   1. Provides the organization with a roadmap for implementing its incident response capability;
   2. Describes the structure and organization of the incident response capability;
   3. Provides a high-level approach for how the incident response capability fits into the overall organization;
   4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   5. Defines reportable incidents;
   6. Provides metrics for measuring the incident response capability within the organization;
   7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
   8. Addresses the sharing of incident information;
   9. Is reviewed and approved by [*AO, ISSM, ISSO, PM, CISO*] [*annually*]; and
   10. Explicitly designates responsibility for incident response to [*the GSA Incident Response Team*].

b. Distribute copies of the incident response plan to [*AO, ISSM, ISSO, PM, CISO*) and organizational elements];

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to [*AO, ISSM, ISSO, PM, CISO*]; and

e. Protect the incident response plan from unauthorized disclosure and modification.

IR-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented	

IR-8	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-8 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	

13.8.15 IR-8 (1): Incident Response Plan | Breaches

Include the following in the Incident Response Plan for breaches involving personally identifiable information:
(a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
(b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such

harms; and
(c) Identification of applicable privacy requirements.

Note: Only applicable if PII is stored, processed, or transmitted by the system.

IR-8 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
IR-8 (1) Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.9 Maintenance

13.9.1 MA-1: Policy and Procedures

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
   1. [*Organization-level*] maintenance policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and

c. Review and update the current maintenance:

1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

MA-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Maintenance CIO-IT Security-10-50 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MA-1 Describe how the control is implemented.	
Part a	1. The GSA maintenance policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding the maintenance for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Maintenance procedures are documented in CIO-IT Security-10-50, "IT Security Procedural Guide: Maintenance (MA)." The procedures facilitate the implementation of the maintenance policy and associated controls. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.

MA-1	Control Summary Information
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-10-50 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.9.2 MA-2: Controlled Maintenance

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;
c. Require that [*Information System Security Manager, Information System Security Officer, System Owners, Custodians*] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;
d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [*Controlled Unclassified Information, system configuration information (e.g., account names, internal IP addresses, etc.)*];
e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
f. Include the following information in organizational maintenance records: [*(1) Date and time of maintenance, (2) Name of the individual performing the maintenance, (3) Name of escort, if necessary, (4) A description of the maintenance performed, (5) A list of equipment removed or replaced (including identification numbers, if applicable)*].

MA-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

MA-2	Control Summary Information
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MA-2 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	

13.9.3 MA-3: Maintenance Tools

a. Approve, control, and monitor the use of system maintenance tools; and
b. Review previously approved system maintenance tools [*annually as part of CM Plan review*].

MA-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MA-3 Describe how the control is implemented.	
Part a	
Part b	

13.9.4 MA-3 (1): Maintenance Tools | Inspect Tools

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

MA-3 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP)	

MA-3 (1)	Control Enhancement Summary Information
☐ System Specific Control	
MA-3 (1) Describe how the control is implemented.	

13.9.5 MA-3 (2): Maintenance Tools | Inspect Media

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

MA-3 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MA-3 (2) Describe how the control is implemented.	

13.9.6 MA-3 (3): Maintenance Tools | Prevent Unauthorized Removal

Prevent the removal of maintenance equipment containing organizational information by:
(a) Verifying that there is no organizational information contained on the equipment;
(b) Sanitizing or destroying the equipment;
(c) Retaining the equipment within the facility; or
(d) Obtaining an exemption from [*Information System Security Manager, Information System Security Officer, System Owners, Custodians*] explicitly authorizing removal of the equipment from the facility.

MA-3 (3)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MA-3 (3) Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

13.9.7 MA-4: Nonlocal Maintenance

a. Approve and monitor nonlocal maintenance and diagnostic activities;
b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintain records for nonlocal maintenance and diagnostic activities; and
e. Terminate session and network connections when nonlocal maintenance is completed.

MA-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MA-4 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	

13.9.8 MA-5: Maintenance Personnel

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and
c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

MA-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MA-5 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.9.9 MA-6: Timely Maintenance

Obtain maintenance support and/or spare parts for [*GSA S/SO or Contractor recommended information system components to be approved by the GSA CISO and AO*] within [*a time period as determined by the Contingency Plan and BIA*] of failure.

MA-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MA-6 Describe how the control is implemented.	

13.10 Media Protection

13.10.1 MP-1: Policy and Procedures

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

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the media protection policy and procedures; and

c. Review and update the current media protection:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

MP-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Media Protection CIO-IT Security-06-32 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MP-1 Describe how the control is implemented.	
Part a	1. The GSA media protection policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding the media protection for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Media protection procedures are documented in CIO-IT Security-06-32, "IT Security Procedural Guide: Media Protection (MP)." The procedures facilitate the implementation of the media protection policy and associated controls. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-06-32 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.10.2 MP-2: Media Access

Restrict access to [*S/SO or Contractor recommended and GSA CISO and AO approved types of digital and/or non-digital media*] to [*S/SO or Contractor recommended and GSA CISO and AO*

approved personnel or roles].

MP-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MP-2 Describe how the control is implemented.	

13.10.3 MP-3: Media Marking

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempt [*no media (i.e., all media must be marked)*] from marking if the media remain within [*all environments, including controlled areas*].

MP-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

MP-3	Control Summary Information
MP-3 Describe how the control is implemented.	
Part a	
Part b	

13.10.4 MP-4: Media Storage

a. Physically control and securely store [*digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, and disks of any type and non-digital media*] within [*locked cabinets or safes in secure/controlled facilities within the authorization boundary*]; and
b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

MP-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MP-4 Describe how the control is implemented.	
Part a	

MP-4	Control Summary Information
Part b	

13.10.5 MP-5: Media Transport

a. Protect and control [*digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, and disks of any type*] during transport outside of controlled areas using [*a FIPS 140-2 validated encryption module/mechanism*];
b. Maintain accountability for system media during transport outside of controlled areas;
c. Document activities associated with the transport of system media; and
d. Restrict the activities associated with the transport of system media to authorized personnel.

MP-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MP-5 Describe how the control is implemented.	
Part a	
Part b	

MP-5	Control Summary Information
Part c	
Part d	

13.10.6 MP-6: Media Sanitization

a. Sanitize [*all information system media, both digital and non-digital*] prior to disposal, release out of organizational control, or release for reuse using [*GSA S/SO or Contractor recommended and GSA CISO and AO approved sanitization techniques and procedures*]; and
b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

MP-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MP-6 Describe how the control is implemented.	
Part a	
Part b	

13.10.7 MP-7: Media Use

a. [*Restricts*] the use of [digital storage devices, including backup media, removable media, and mobile devices] on [*GSA information systems*] using [*GSA S/SO recommended and GSA CISO and AO approved security safeguards*]; and

b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

MP-7	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
MP-7 Describe how the control is implemented.	
Part a	
Part b	

13.11 Physical and Environmental Protection

13.11.1 PE-1: Policy and Procedures

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
   1. [*Organization-level*] physical and environmental protection policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:

1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

PE-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Physical and Environmental Protection CIO-IT Security-12-64 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-1 Describe how the control is implemented.	
Part a	1. The GSA physical and environmental protection policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding the physical and environmental protection for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Media protection procedures are documented in CIO-IT Security-12-64, "IT Security Procedural Guide: Physical and Environmental Protection (PE)." The procedures facilitate the implementation of the physical and environmental protection policy and associated controls. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.

PE-1	Control Summary Information
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-12-64 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.11.2 PE-2: Physical Access Authorizations

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;
b. Issue authorization credentials for facility access;
c. Review the access list detailing authorized facility access by individuals [*at least annually*]; and
d. Remove individuals from the facility access list when access is no longer required.

PE-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-2 Describe how the control is implemented.	
Part a	

PE-2	Control Summary Information
Part b	
Part c	
Part d	

13.11.3 PE-3: Physical Access Control

a. Enforce physical access authorizations at [*GSA S/SO or Contractor recommended and GSA CISO and AO approved entry/exit points to the facility where the information system resides*] by:

   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress and egress to the facility using [*Physical Access Control Systems (PACS) devices IAW GSA Order ADM 5900.1, and guards for on-premises contracts; GSA S/SO or Contractor recommended and GSA CISO and AO approved physical access control systems, devices, guards for off-premises contracts*];

b. Maintain physical access audit logs for [*GSA S/SO or Contractor recommended entry/exit points approved by the GSA CISO and AO*];

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [*GSA S/SO or Contractor recommended physical access controls approved by the GSA CISO and AO*];

d. Escort visitors and control visitor activity [*GSA S/SO or Contractor recommended circumstances requiring visitor escorts and monitoring approved by the GSA CISO and AO*];

e. Secure keys, combinations, and other physical access devices;

f. Inventory [*GSA S/SO or Contractor recommended physical access devices approved by the GSA CISO and AO*] every [*year*]; and

g. Change combinations and keys [*at least annually*] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

PE-3	Control Summary Information

Implementation Status:

☐ Implemented
☐ Partially Implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

Control Origination:

☐ Inherited from: [Enter System's Name]
☐ [Source System's Name] Common Control
☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP)
☐ System Specific Control

PE-3 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	

PE-3	Control Summary Information
Part g	

13.11.4 PE-4: Access Control for Transmission

Control physical access to [*GSA S/SO or Contractor recommended and GSA CISO and AO approved information system distribution and transmission lines*] within organizational facilities using [*GSA S/SO or Contractor recommended and GSA CISO and AO approved security controls*].

PE-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-4 Describe how the control is implemented.	

13.11.5 PE-5: Access Control for Output Devices

Control physical access to output from [*all IT assets*] to prevent unauthorized individuals from obtaining the output.

PE-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

PE-5	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-5 Describe how the control is implemented.	

13.11.6 PE-6: Monitoring Physical Access

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;
b. Review physical access logs [*at least annually*] and upon occurrence of [*physical security incidents*]; and
c. Coordinate results of reviews and investigations with the organizational incident response capability.

PE-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-6 Describe how the control is implemented.	

PE-6	Control Summary Information
Part a	
Part b	
Part c	

13.11.7 PE-6 (1): Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

PE-6 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-6 (1) Describe how the control is implemented.	

13.11.8 PE-8: Visitor Access Records

a. Maintain visitor access records to the facility where the system resides for [*GSA S/SO or Contractor recommended and GSA CISO and AO approved time period*];
b. Review visitor access records [*at least annually*]; and
c. Report anomalies in visitor access records to [*ISSO, ISSM, and facility security staff (e.g., Federal Protective Service)*].

PE-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-8 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.11.9 PE-8 (3): Visitor Access Records | Limit Personally Identifiable Information Elements

Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: [*individual visitor's name*].

PE-8 (3)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-8 (3) Describe how the control is implemented.	

13.11.10 PE-9: Power Equipment and Cabling

Protect power equipment and power cabling for the system from damage and destruction.

PE-9	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

PE-9	Control Summary Information
PE-9 Describe how the control is implemented.	

13.11.11 PE-10: Emergency Shutoff

a. Provide the capability of shutting off power to [*any physical equipment*] in emergency situations;
b. Place emergency shutoff switches or devices in [*GSA S/SO or Contractor recommended and GSA CISO and AO approved location by information system or system component*] to facilitate access for authorized personnel; and
c. Protect emergency power shutoff capability from unauthorized activation.

PE-10	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-10 Describe how the control is implemented.	
Part a	
Part b	

PE-10	Control Summary Information
Part c	

13.11.12 PE-11: Emergency Power

Provide an uninterruptible power supply to facilitate [*an orderly shutdown of the information system; transition of the information system to long-term alternate power*] in the event of a primary power source loss.

PE-11	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-11 Describe how the control is implemented.	

13.11.13 PE-12: Emergency Lighting

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

PE-12	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented	

PE-12	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-12 Describe how the control is implemented.	

13.11.14 PE-13: Fire Protection

Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

PE-13	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-13 Describe how the control is implemented.	

13.11.15 PE-13 (1): Fire Protection | Detection Systems – Automatic Activation and Notification

Employ fire detection systems that activate automatically and notify [*Information System Security Officer, System Owners, Acquisitions/Contracting Officers, Custodians*] and [*Police and Fire Department*] in the event of a fire.

PE-13 (1)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-13 (1) Describe how the control is implemented.	

13.11.16 PE-14: Environmental Controls

a. Maintain [*temperature; humidity*] levels within the facility where the system resides at [*Data center temperature range (taken at the server inlets) should be 18 degrees Celsius to 27 degrees (64.4 degrees Fahrenheit to 80.6 degrees). Data center humidity levels (measured by dew point) should be within 5.5 degrees Celsius to 15 degrees (41.9 degrees Fahrenheit to 59 degrees). Ranges are consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) guidelines*]; and
b. Monitor environmental control levels [*continuously*].

PE-14	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

PE-14	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-14 Describe how the control is implemented.	
Part a	
Part b	

13.11.17 PE-15: Water Damage Protection

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

PE-15	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

PE-15	Control Summary Information
PE-15 Describe how the control is implemented.	

13.11.18 PE-16: Delivery and Removal

a. Authorize and control [*all information system components*] entering and exiting the facility; and
b. Maintain records of the system components.

PE-16	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-16 Describe how the control is implemented.	

13.11.19 PE-17: Alternate Work Site

a. Determine and document the [*GSA S/SO or Contractor defined and GSA CISO and AO approved alternate work sites*] allowed for use by employees;
b. Employ the following controls at alternate work sites: [*security control requirements as identified in GSA Order ADM 2450.1*];
c. Assess the effectiveness of controls at alternate work sites; and
d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

PE-17	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PE-17 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

13.12 Planning

13.12.1 PL-1: Policy and Procedures

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
   1. [*Organization-level*] planning policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the planning policy and procedures; and

c. Review and update the current planning:

1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

PL-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk Security Assessment and Authorization, Planning, and Risk Assessment (CA, PL, & RA) CIO-IT Security-06-30 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PL-1 Describe how the control is implemented.	
Part a	1. The GSA security planning policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding the security planning for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Planning procedures are documented in CIO-IT Security-06-30, "IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk." The procedures facilitate the implementation of the security planning policy and associated controls. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.

PL-1	Control Summary Information
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-06-30 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.12.2 PL-2: System Security and Privacy Plans

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

b. Distribute copies of the plans and communicate subsequent changes to the plans to [*defined in GSA CIO Order 2100.1*];

c. Review the plans [*annually*];

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

PL-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PL-2 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	

13.12.3 PL-4: Rules of Behavior

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

PL-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PL-4 Describe how the control is implemented.	
Part a	
Part b	
Part c	

PL-4	Control Summary Information
Part d	

13.12.4 PL-4 (1): Rules of Behavior | Social Media and External Site/Application Usage Restrictions

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

PL-4 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PL-4 (1) Describe how the control is implemented.	

13.12.5 PL-8: Security and Privacy Architectures

a. Develop security and privacy architectures for the system that:
1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;

3. Describe how the architectures are integrated into and support the enterprise architecture; and

4. Describe any assumptions about, and dependencies on, external systems and services;

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

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

PL-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PL-8 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.12.6 PL-9: Central Management

Centrally manage [*common and hybrid security and privacy controls as identified in CIO-IT Security-18-90, Information Security Program Plan (ISPP)*].

PL-9	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PL-9 Describe how the control is implemented.	

13.12.7 PL-10: Baseline Selection

Select a control baseline for the system.

PL-10	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

PL-10	Control Summary Information
PL-10 Describe how the control is implemented.	

13.12.8 PL-11: Baseline Tailoring

Tailor the selected control baseline by applying specified tailoring actions.

PL-11	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PL-11 Describe how the control is implemented.	

13.13 Personnel Security

13.13.1 PS-1: Policy and Procedures

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

2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

PS-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and Personnel Security Handbook (ADM 9732.1) ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PS-1 Describe how the control is implemented.	
Part a	1. The GSA personnel security policy is defined in the GSA IT Security Policy, CIO 2100.1, GSA Order ADM 9732.1, "Personnel Security and Suitability Program Handbook" and GSA Order ADM 2181.1, "Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors." which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for personnel security activities. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Personnel security procedures are documented in CIO-IT Security-03-23, "IT Security Procedural Guide: Termination and Transfer" and in CIO-IT Security-18-90, "IT Security Procedural Guide: Information Security Program Plan (ISPP)." These procedures facilitate the implementation of the personnel security policy

PS-1	Control Summary Information
	and associated controls. The guides and policies are disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-03-23 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.13.2 PS-2: Position Risk Designation

a. Assign a risk designation to all organizational positions;
b. Establish screening criteria for individuals filling those positions; and
c. Review and update position risk designations [*as necessary, to meet changing roles, responsibilities and Federal requirements*].

PS-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PS-2 Describe how the control is implemented.	
Part a	

PS-2	Control Summary Information
Part b	
Part c	

13.13.3 PS-3: Personnel Screening

a. Screen individuals prior to authorizing access to the system; and
b. Rescreen individuals in accordance with [*requirements specified in GSA Orders CIO 2100.1, ADM 2181.1, ADM 9732.1*].

PS-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PS-3 Describe how the control is implemented.	
Part a	
Part b	

13.13.4 PS-4: Personnel Termination

Upon termination of individual employment:

a. Disable system access within [*30 days of personnel termination*];
b. Terminate or revoke any authenticators and credentials associated with the individual;
c. Conduct exit interviews that include a discussion of [*privacy, disclosure, and confidentiality responsibilities*];
d. Retrieve all security-related organizational system-related property; and
e. Retain access to organizational information and systems formerly controlled by terminated individual.

PS-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PS-4 Describe how the control is implemented.	
Part a	
Part b	
Part c	

PS-4	Control Summary Information
Part d	
Part e	

13.13.5 PS-5: Personnel Transfer

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiate [*denial or modification of access privileges to specific information systems based on their new duties*] within [*30 days of personnel transfer*];
c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notify [*supervisor and/or ISSMs/ISSOs*] within [*14 days of personnel transfer*].

PS-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PS-5 Describe how the control is implemented.	
Part a	

PS-5	Control Summary Information
Part b	
Part c	
Part d	

13.13.6 PS-6: Access Agreements

a. Develop and document access agreements for organizational systems;
b. Review and update the access agreements [*annually*]; and
c. Verify that individuals requiring access to organizational information and systems:
   1. Sign appropriate access agreements prior to being granted access; and
   2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [*at least annually*]

PS-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PS-6 Describe how the control is implemented.	

PS-6	Control Summary Information
Part a	
Part b	
Part c	

13.13.7 PS-7: External Personnel Security

a. Establish personnel security requirements, including security roles and responsibilities for external providers;
b. Require external providers to comply with personnel security policies and procedures established by the organization;
c. Document personnel security requirements;
d. Require external providers to notify [*the Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [*the same day*]; and
e. Monitor provider compliance with personnel security requirements.

PS-7	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

PS-7	Control Summary Information
PS-7 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	

13.13.8 PS-8: Personnel Sanctions

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and
b. Notify [*the Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*] within [*the same day*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

PS-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

PS-8	Control Summary Information
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PS-8 Describe how the control is implemented.	
Part a	
Part b	

13.13.9 PS-9: Position Descriptions

Incorporate security and privacy roles and responsibilities into organizational position descriptions.

PS-9	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PS-9 Describe how the control is implemented.	

13.14 Personally Identifiable Information Processing and Transparency

Note: Only applicable if PII is stored, processed, or transmitted by the system.

13.14.1 PT-1: Policy and Procedures

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

b. Designate an [*Chief Privacy Officer*] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and

c. Review and update the current personally identifiable information processing and transparency:
   1. Policy [*annually, as part of a Privacy Program review*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

PT-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA's Privacy Program and policies (see Privacy InSite page) ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

PT-1	Control Summary Information
PT-1 Describe how the control is implemented.	
Part a	1. The GSA Privacy Office develops, disseminates, and implements operational privacy policies and that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII. They are disseminated via the Privacy InSite page. (a) The policies and procedures on the Privacy page address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (b) The Privacy policies, procedures, and processes are consistent with Federal laws, orders, directives, regulations, policies, standards, and guidelines. 2. The GSA Privacy Office develops, disseminates, and implements operational privacy procedures (e.g., PTA and PIA processes) via the Privacy InSite page that provide guidance for processing PII and complying with associated privacy controls.
Part b	GSA has a designated Chief Privacy Officer (CPO) (and Senior Agency Official for Privacy [SAOP]) and allocates sufficient resources to implement and operate the organization-wide privacy program. The CPO leads the GSA Privacy Office which develops privacy policies and manages the GSA privacy program.
Part c	1. The GSA Privacy Office develops, disseminates, and implements operational privacy policies and that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII in accordance with Federal laws, policies, and requirements. They are reviewed on an annual basis and updated as necessary. 2. The GSA Privacy Office develops, disseminates, and implements operational privacy procedures (e.g., PTA and PIA processes) that provide guidance for identifying and safeguarding PII. They are reviewed on an annual basis and updated as necessary.

13.14.2 PT-2: Authority to Process Personally Identifiable Information

a. Determine and document the [*authority as defined in the SORN*] that permits the [*processing as defined in the SORN*] of personally identifiable information; and
b. Restrict the [*processing as defined in the SORN*] of personally identifiable information to only that which is authorized.

PT-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PT-2 Describe how the control is implemented.	
Part a	
Part b	

13.14.3 PT-3: Personally Identifiable Information Processing Purposes

a. Identify and document the [*purposes in the SORN*] for processing personally identifiable information;
b. Describe the purpose(s) in the public privacy notices and policies of the organization;
c. Restrict the [*processing*] of personally identifiable information to only that which is compatible with the identified purpose(s); and
d. Monitor changes in processing personally identifiable information and implement [*PTA, PIA and SORN processes*] to ensure that any changes are made in accordance with [*CIO Order 1878.3*].

PT-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation	

PT-3	Control Summary Information
☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PT-3 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

13.14.4 PT-4: Consent

Implement [*Privacy Act statements*] for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.

PT-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

PT-4	Control Summary Information
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PT-4 Describe how the control is implemented.	

13.14.5 PT-5: Privacy Notice

Provide notice to individuals about the processing of personally identifiable information that:

a. Is available to individuals upon first interacting with an organization, and subsequently at [*whenever PII is collected, updated or disclosed*];
b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;
c. Identifies the authority that authorizes the processing of personally identifiable information;
d. Identifies the purposes for which personally identifiable information is to be processed; and
e. Includes [*PII as defined in https://docs.google.com/spreadsheets/d/1Yb9I9C3qCee8dnkVIIUqIZgrWsA1DoW0xYF2yPjgz0I/edit#gid=1521803081*].

PT-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

PT-5	Control Summary Information
PT-5 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	

13.14.6 PT-5 (2): Privacy Notice | Privacy Act Statements

Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

PT-5 (2)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's	

PT-5 (2)	Control Summary Information
Name] SSPP) ☐ System Specific Control	
PT-5 (2) Describe how the control is implemented.	

13.14.7 PT-6: System of Records Notice

For systems that process information that will be maintained in a Privacy Act system of records:

a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;
b. Publish system of records notices in the Federal Register; and
c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

PT-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PT-6 Describe how the control is implemented.	
Part a	

PT-6	Control Summary Information
Part b	
Part c	

13.14.8 PT-6 (1): System of Records Notice | Routine Uses

Review all routine uses published in the system of records notice at [*any major change or every two years*] to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.

PT-6 (1)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PT-6 (1) Describe how the control is implemented.	

13.14.9 PT-6 (2): System of Records Notice | Exemption Rules

Review all Privacy Act exemptions claimed for the system of records at [*any major change or every two years*] to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.

PT-6 (2)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PT-6 (2) Describe how the control is implemented.	

13.14.10 PT-7: Specific Categories of Personally Identifiable Information

Apply *[FIPS-validated encryption]* for specific categories of personally identifiable information.

PT-7	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

PT-7	Control Summary Information
PT-7 Describe how the control is implemented.	

13.14.11 PT-7 (1): Specific Categories of Personally Identifiable Information | Social Security Numbers

When a system processes Social Security numbers:

(a) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;
(b) Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and
(c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

PT-7 (1)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PT-7 (1) Describe how the control is implemented.	
Part a	

PT-7 (1)	Control Summary Information
Part b	
Part c	

13.14.12 PT-7 (2): Specific Categories of Personally Identifiable Information | First Amendment Information

Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

PT-7 (2)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PT-7 (2) Describe how the control is implemented.	

13.14.13 PT-8: Computer Matching Requirements

When a system or organization processes information for the purpose of conducting a matching program:

a. Obtain approval from the Data Integrity Board to conduct the matching program;

b. Develop and enter into a computer matching agreement;
c. Publish a matching notice in the Federal Register;
d. Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and
e. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

PT-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
PT-8 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

PT-8	Control Summary Information
Part e	

13.15 Risk Assessment

13.15.1 RA-1: Policy and Procedures

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

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

c. Review and update the current risk assessment:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

RA-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk Security Assessment and Authorization, Planning, and Risk Assessment (CA, PL, & RA), CIO-IT Security-06-30 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP)	

RA-1	Control Summary Information
☐ System Specific Control	
RA-1 Describe how the control is implemented.	
Part a	1. The GSA risk assessment policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for risk assessment activities. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Risk assessment procedures are documented in CIO-IT Security-06-30, "IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk." The procedures facilitate the implementation of the risk assessment policy and associated controls. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-06-30 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.15.2 RA-2: Security Categorization

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

RA-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

RA-2	Control Summary Information
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
RA-2 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.15.3 RA-3: Risk Assessment

a. Conduct a risk assessment, including:

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

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in [*a security assessment report (SAR) or as specified in CIO-IT Security-06-30 and GSA's other Assessment and Authorization processes identified therein*];

d. Review risk assessment results [*as specified in CIO-IT Security-06-30 and GSA's other Assessment and Authorization processes identified therein*];

e. Disseminate risk assessment results to [*personnel with risk assessment/management responsibilities as defined in GSA CIO Order 2100.1*];

and
f. Update the risk assessment [*as specified in CIO-IT Security-06-30 and GSA's other Assessment and Authorization processes identified therein*] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

RA-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
RA-3 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

RA-3	Control Summary Information
Part e	
Part f	

13.15.4 RA-3 (1): Risk Assessment | Supply Chain Risk Assessment

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

RA-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
RA-3 Describe how the control is implemented.	
Part a	

RA-3	Control Summary Information
Part b	

13.15.5 RA-5: Vulnerability Monitoring and Scanning

a. Monitor and scan for vulnerabilities in the system and hosted applications [*weekly authenticated scans for operating systems (OS)-including databases, monthly unauthenticated scans for web application, annual authenticated scans for web applications*] and when new vulnerabilities potentially affecting the system are identified and reported;
b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations;
   2. Formatting checklists and test procedures; and
   3. Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from vulnerability monitoring;
d. Remediate legitimate vulnerabilities [
   (1) BOD Timelines
      (a) Within 14 days for vulnerabilities added to CISA's KEV Catalog with a CVE date post FY21.
      (b) Per the CISA KEV catalog date or GSA Standard timelines below, whichever is earlier, for vulnerabilities in the CISA KEV catalog with a CVE date in FY21 or earlier.
      (c) Within 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.
   (2) GSA Standard Timelines
      (a) Within 30 days for Critical (Very High) and High vulnerabilities.
      (b) Within 90 days for Moderate vulnerabilities.
      (c) Within 120 days for Low vulnerabilities for Internet-accessible systems/services.]
   in accordance with an organizational assessment of risk;
e. Share information obtained from the vulnerability monitoring process and control assessments with [*Information System Security Officers*] to help eliminate similar vulnerabilities in other systems; and
f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

RA-5	Control Summary Information
Implementation Status: ☐ Implemented	

RA-5	Control Summary Information
☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
RA-5 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	

13.15.6 RA-5 (2): Vulnerability Monitoring and Scanning | Update Vulnerabilities to be Scanned

Update the system vulnerabilities to be scanned [*continuously - before each scan*].

RA-5 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
RA-5 (2) Describe how the control is implemented.	

13.15.7 RA-5 (5): Vulnerability Monitoring and Scanning | Privileged Access

Implement privileged access authorization to [*all information system components as applicable (e.g., OS, DB, Web App, etc.*] for [*all vulnerability scanning activities*].

RA-5 (5)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP)	

RA-5 (5)	Control Enhancement Summary Information
☐ System Specific Control	
RA-5 (5) Describe how the control is implemented.	

13.15.8 RA-5 (11): Vulnerability Monitoring and Scanning | Public Disclosure Program

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

RA-5 (11)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
RA-5 (11) Describe how the control is implemented.	

13.15.9 RA-7: Risk Response

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

RA-7	Control Enhancement Summary Information
Implementation Status: ☐ Implemented	

RA-7	Control Enhancement Summary Information
☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
RA-7 Describe how the control is implemented.	

13.15.10 RA-8: Privacy Impact Assessments

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

Note: RA-8 is included in all FIPS 199 Baselines to ensure all systems complete a Privacy Threshold Assessment (PTA) to determine if a Privacy Impact Assessment (PIA) is required. If the PTA determines a PIA is not required mark RA-8 as "Implemented" and state in parts a and b "PTA completed, a PIA is not required."

RA-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

RA-8	Control Summary Information
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
RA-8 Describe how the control is implemented.	
Part a	
Part b	

13.15.11 RA-9: Criticality Analysis

Identify critical system components and functions by performing a criticality analysis for [*GSA S/SO or Contractor recommended and AO approved systems, system components, or system services*] at [*the implementation phase and if there are significant changes modifying criticality during the operations and maintenance phase*].

RA-9	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
RA-9 Describe how the control is implemented.	

RA-9	Control Enhancement Summary Information

13.16 System and Services Acquisition

13.16.1 SA-1: Policy and Procedures

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

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

c. Review and update the current system and services acquisition:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

SA-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Security and Privacy Requirements for IT Acquisition Efforts CIO-IT Security-09-48 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

SA-1	Control Summary Information
SA-1 Describe how the control is implemented.	
Part a	1. The GSA system and services acquisition policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for system and services acquisition activities. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. System and services acquisition procedures are documented in CIO-IT Security-09-48, "IT Security Procedural Guide: Security and Privacy Requirements for IT Acquisition Efforts." The procedures facilitate the implementation of the system and services acquisition policy and associated controls. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-09-48 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.16.2 SA-2: Allocation of Resources

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;
b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and
c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

SA-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

SA-2	Control Summary Information
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-2 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.16.3 SA-3: System Development Life Cycle

a. Acquire, develop, and manage the system using [the GSA Solutions Lifecycle (SLC)] that incorporates information security and privacy considerations;
b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;
c. Identify individuals having information security and privacy roles and responsibilities; and
d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

SA-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name]	

SA-3	Control Summary Information
☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-3 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

13.16.4 SA-3 (2): System Development Life Cycle | Use of Live or Operational Data

(a) Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and
(b) Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.

SA-3 (2)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name]	

SA-3 (2)	Control Summary Information
☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-3 (2) Describe how the control is implemented.	
Part a	
Part b	

13.16.5 SA-4: Acquisition Process

Include the following requirements, descriptions, and criteria, explicitly or by reference, using [*standardized contract language per CIO-IT Security-09-48, Security and Privacy Requirements for IT Acquisition Efforts*] in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;
b. Strength of mechanism requirements;
c. Security and privacy assurance requirements;
d. Controls needed to satisfy the security and privacy requirements.
e. Security and privacy documentation requirements;
f. Requirements for protecting security and privacy documentation;
g. Description of the system development environment and environment in which the system is intended to operate;
h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and
i. Acceptance criteria.

SA-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

SA-4	Control Summary Information
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-4 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	

SA-4	Control Summary Information
Part h	
Part i	

13.16.6 SA-4 (1): Acquisition Process | Functional Properties of Controls

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

SA-4 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-4 (1) Describe how the control is implemented.	

13.16.7 SA-4 (2): Acquisition Process | Design and Implementation Information for Controls

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [*GSA S/SO or Contractor recommended security-relevant external system interfaces and design/implementation detail(s) as approved by the GSA CISO and AO*] at [*GSA S/SO or Contractor recommended level of detail as approved by the GSA CISO and AO*].

SA-4 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-4 (2) Describe how the control is implemented.	

13.16.8 SA-4 (9): Acquisition Process | Functions, Ports, Protocols, and Services in Use

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

SA-4 (9)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-4 (9) Describe how the control is implemented.	

SA-4 (9)	Control Enhancement Summary Information

13.16.9 SA-4 (10): Acquisition Process | Use of Approved PIV Products

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

SA-4 (10)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-4 (10) Describe how the control is implemented.	

13.16.10 SA-5: System Documentation

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

1. Secure configuration, installation, and operation of the system, component, or service;
2. Effective use and maintenance of security and privacy functions and mechanisms; and
3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [*GSA S/SO or Contractor recommended actions as approved by the GSA CISO and AO*] in response; and

d. Distribute documentation to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*].

SA-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-5 Describe how the control is implemented.	
Part a	
Part b	
Part c	

SA-5	Control Summary Information
Part d	

13.16.11 SA-8: Security and Privacy Engineering Principles

Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [*the review defined in CIO-IT Security-19-195, Security Engineering Architecture Reviews*].

SA-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-8 Describe how the control is implemented.	

13.16.12 SA-8 (33): Security and Privacy Engineering Principles | Minimization

Implement the privacy principle of minimization using [*PTA, PIA, SORN, and records schedules*].

Note: Only applicable if PII is stored, processed, or transmitted by the system.

SA-8 (33)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented	

SA-8 (33)	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-8 (33) Describe how the control is implemented.	

13.16.13 SA-9: External Information System Services

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [*FISMA, OMB, NIST, and GSA defined security controls*];
b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and
c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: *[contract language and service level agreements*]

SA-9	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

SA-9	Control Summary Information
SA-9 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.16.14 SA-9 (2): External System Services | Identification of Functions, Ports, Protocols, and Services

Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [*GSA S/SO or Contractor recommended external information system services as approved by the GSA CISO and AO*].

SA-9 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-9 (2) Describe how the control is implemented.	

13.16.15 SA-10: Developer Configuration Management

Require the developer of the system, system component, or system service to:
a. Perform configuration management during system, component, or service [*design, development, implementation, operations, and disposal*];
b. Document, manage, and control the integrity of changes to *[(1) Configuration items identified in the system configuration management plan, (2) GSA S/SO recommended and AO approved configuration items for systems without a configuration management plan*];
c. Implement only organization-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to [*the Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*].

SA-10	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-10 Describe how the control is implemented.	
Part a	
Part b	

SA-10	Control Summary Information
Part c	
Part d	
Part e	

13.16.16 SA-11: Developer Testing and Evaluation

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:
a. Develop and implement a plan for ongoing security and privacy control assessments;
b. Perform [*GSA S/SO or Contractor recommended and GSA CISO and AO approved (e.g., unit, integration, system, regression)*] testing/evaluation [*during A&A assessments and prior to a new code release*] at [*GSA S/SO or Contractor recommended and GSA CISO and AO approved depth and coverage*];
c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during testing and evaluation.

SA-11	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

SA-11	Control Summary Information
SA-11 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	

13.16.17 SA-11 (1): Developer Testing and Evaluation | Static Code Analysis

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

Note: Applicable only if system is internet accessible

SA-11 (1)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control	

SA-11 (1)	Control Summary Information
☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-11 (1) Describe how the control is implemented.	

13.16.18 SA-15: Development Process, Standards, and Tools

a. Require the developer of the system, system component, or system service to follow a documented development process that:
   1. Explicitly addresses security and privacy requirements;
   2. Identifies the standards and tools used in the development process;
   3. Documents the specific tool options and tool configurations used in the development process; and
   4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Review the development process, standards, tools, tool options, and tool configurations [*GSA S/SO or Contractor recommended and GSA CISO and AO approved frequency*] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [*GSA S/SO or Contractor recommended and GSA CISO and AO approved security and privacy requirements*].

SA-15	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

SA-15	Control Summary Information
SA-15 Describe how the control is implemented.	
Part a	
Part b	

13.16.19 SA-15 (3): Development Process, Standards, and Tools | Criticality Analysis

Require the developer of the system, system component, or system service to perform a criticality analysis:

(a) At the following decision points in the system development life cycle: [*prior to being placed into production*]; and

(b) At the following level of rigor: [*GSA S/SO or Contractor recommended and GSA CISO and AO approved depth of criticality analysis*].

SA-15 (3)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-15 (3) Describe how the control is implemented.	
Part a	

SA-15 (3)	Control Summary Information
Part b	

13.16.20 SA-22: Unsupported System Components

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or
b. Provide the following options for alternative sources for continued support for unsupported components [*none (requires an approved Acceptance of Risk Letter)*].

SA-22	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SA-22 Describe how the control is implemented.	
Part a	
Part b	

13.17 System and Communications Protection

13.17.1 SC-1: Policy and Procedures

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

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

c. Review and update the current system and communications protection:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

SC-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and applicable technical guides located on the IT Security Technical Guides and Standard webpage (https://insite.gsa.gov/employee-resources/information-technology/security-and-privacy/it-security/it-security-technical-guides-and-standards): ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-1 Describe how the control is implemented.	
Part a	1. The GSA system and communications protection policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for system and communications protection activities.

SC-1	Control Summary Information
	This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. GSA OCISO ISP in collaboration with ISE and the Security Operations Division (ISO) has developed a number of technical and procedural guides addressing securely configuring components, access control, key management, firewall changes, etc. which address procedures involving systems and communication protection. These guides are disseminated GSA-wide via a centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. Technical and procedural guides every three years and following changes to Federal or GSA policies. SC controls are covered in multiple procedural guides.

13.17.2 SC-2: Separation of System and User Functionality

Separate user functionality, including user interface services, from system management functionality.

SC-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

SC-2	Control Summary Information
SC-2 Describe how the control is implemented.	

13.17.3 SC-4: Information in Shared System Resources

Prevent unauthorized and unintended information transfer via shared system resources.

SC-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-4 Describe how the control is implemented.	

13.17.4 SC-5: Denial of Service Protection

a. [*Protect against*] the effects of the following types of denial-of-service events: [*network flooding attacks*]; and
b. Employ the following controls to achieve the denial-of-service objective: [*perimeter and internal protection devices/techniques*].

SC-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented	

SC-5	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-5 Describe how the control is implemented.	

13.17.5 SC-7: Boundary Protection

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [*logically*] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

SC-7	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-7 Describe how the control is implemented.	

SC-7	Control Summary Information
Part a	
Part b	
Part c	

13.17.6 SC-7 (3): Boundary Protection | Access Points

Limit the number of external network connections to the system.

SC-7 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-7 (3) Describe how the control is implemented.	

13.17.7 SC-7 (4): Boundary Protection | External Telecommunication Services

(a) Implement a managed interface for each external telecommunication service;
(b) Establish a traffic flow policy for each managed interface;

(c) Protect the confidentiality and integrity of the information being transmitted across each interface;
(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;
(e) Review exceptions to the traffic flow policy [*annually*] and remove exceptions that are no longer supported by an explicit mission or business need;
(f) Prevent unauthorized exchange of control plane traffic with external networks;
(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
(h) Filter unauthorized control plane traffic from external networks.

SC-7 (4)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-7 (4) Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

SC-7 (4)	Control Enhancement Summary Information
Part e	
Part f	
Part g	
Part h	

13.17.8 SC-7 (5): Boundary Protection | Deny by Default - Allow by Exception

Deny network communications traffic by default and allow network communications traffic by exception [*at managed interfaces*].

SC-7 (5)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-7 (5) Describe how the control is implemented.	

13.17.9 SC-7 (7): Boundary Protection | Split Tunneling for Remote Devices

Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [*approved port access requirements and implemented managed firewall*].

SC-7 (7)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-7 (7) Describe how the control is implemented.	

13.17.10 SC-7 (8): Boundary Protection | Route Traffic To Authenticated Proxy Servers

Route [*GSA S/SO or Contractor recommended and GSA CISO and AO approved internal communications traffic*] to [*GSA S/SO or Contractor recommended and GSA CISO and AO approved external networks*] through authenticated proxy servers at managed interfaces.

SC-7 (8)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control	

SC-7 (8)	Control Summary Information
☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-7 (8) Describe how the control is implemented.	

13.17.11 SC-7 (10): Boundary Protection | Prevent Exfiltration

(a) Prevent the exfiltration of information; and
(b) Conduct exfiltration tests [*annually or during A&A of external systems*]

SC-7 (10)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-7 (10) Describe how the control is implemented.	
Part a	
Part b	

13.17.12 SC-7 (24): Boundary Protection | Personally Identifiable Information

For systems that process personally identifiable information:

(a) Apply the following processing rules to data elements of personally identifiable information: [*only as authorized by the Privacy Act of 1974, the relevant SORN, GSA's Data Release Policy and any other applicable law, regulation, or government-wide policy*];
(b) Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;
(c) Document each processing exception; and
(d) Review and remove exceptions that are no longer supported.

Note: Only applicable if PII is stored, processed, or transmitted by the system.

SC-7 (24)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-7 (24) Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

13.17.13 SC-8: Transmission Confidentiality and Integrity

Protect the [*confidentiality and integrity*] of transmitted information.

SC-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-8 Describe how the control is implemented.	

13.17.14 SC-8 (1): Transmission Confidentiality and Integrity | Cryptographic Protection

Implement cryptographic mechanisms to [*prevent unauthorized disclosure of information and detect changes to information*] during transmission.

SC-8 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

SC-8 (1)	Control Enhancement Summary Information
SC-8 (1) Describe how the control is implemented.	

13.17.15 SC-10: Network Disconnect

Terminate the network connection associated with a communications session at the end of the session or after [*60 minutes (long running batch jobs and similar operations are not subject to this time limit)*] of inactivity.

SC-10	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-10 Describe how the control is implemented.	

13.17.16 SC-12: Cryptographic Key Establishment and Management

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [*NIST and FIPS requirements for key generation, distribution, storage, access, and destruction*].

SC-12	Control Summary Information
Implementation Status: ☐ Implemented	

SC-12	Control Summary Information
☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-12 Describe how the control is implemented.	

13.17.17 SC-13: Cryptographic Protection

a. Determine the [*cryptographic mechanism used to secure data in transit and at rest (as applicable)*]; and
b. Implement the following types of cryptography required for each specified cryptographic use: [*FIPS-validated or NSA-approved cryptography*].

SC-13	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-13 Describe how the control is implemented.	

SC-13	Control Summary Information
Part a	
Part b	

13.17.18 SC-15: Collaborative Computing Devices and Applications

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [*currently no exceptions*]; and
b. Provide an explicit indication of use to users physically present at the devices.

SC-15	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-15 Describe how the control is implemented.	
Part a	
Part b	

13.17.19 SC-17: Public Key Infrastructure Certificates

a. Issue public key certificates under an [*approved certificate policy compliant with CIO-IT Security-09-43, Key Management*] or obtain public key certificates from an approved service provider; and
b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

SC-17	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-17 Describe how the control is implemented.	
Part a	
Part b	

13.17.20 SC-18: Mobile Code

a. Define acceptable and unacceptable mobile code and mobile code technologies; and
b. Authorize, monitor, and control the use of mobile code within the system.

SC-18	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

SC-18	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-18 Describe how the control is implemented.	
Part a	
Part b	

13.17.21 SC-20: Secure Name/Address Resolution Service (Authoritative Source)

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

SC-20	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP)	

SC-20	Control Summary Information
☐ System Specific Control	
SC-20 Describe how the control is implemented.	
Part a	
Part b	

13.17.22 SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)

Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

SC-21	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-21 Describe how the control is implemented.	

13.17.23 SC-22: Architecture and Provisioning for Name/Address Resolution Service

Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

SC-22	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-22 Describe how the control is implemented.	

13.17.24 SC-23: Session Authenticity

Protect the authenticity of communications sessions.

SC-23	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-23 Describe how the control is implemented.	

SC-23	Control Summary Information

13.17.25 SC-28: Protection of Information at Rest

Protect the [*confidentiality and integrity*] of the following information at rest: *[(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 GSA CISO and AO*].

SC-28	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-28 Describe how the control is implemented.	

13.17.26 SC-28 (1): Protection of Information at Rest | Cryptographic Protection

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [every asset of the system everywhere, including databases and applications]: *[(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 GSA CISO and AO*].

GSA NOTE: For databases, encryption of the whole database, table, column, or field levels is acceptable, as appropriate. Other methods including, but not limited to, application encryption

or tokenization are also acceptable.

SC-28 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-28 (1) Describe how the control is implemented.	

13.17.27 SC-39: Process Isolation

Maintain a separate execution domain for each executing system process.

SC-39	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SC-39 Describe how the control is implemented.	

SC-39	Control Summary Information

13.18 System and Information Integrity

13.18.1 SI-1: Policy and Procedures

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

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

SI-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: System and Information Integrity CIO-IT Security-12-63 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

SI-1	Control Summary Information
SI-1 Describe how the control is implemented.	
Part a	1. The GSA system and information integrity policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for system and information integrity activities. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. System and information integrity procedures are documented in CIO-IT Security-12-63, "IT Security Procedural Guide: System and Information Integrity (SI)." The procedures facilitate the implementation of the system and information integrity policy and associated controls. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-12-63 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.18.2 SI-2: Flaw Remediation

a. Identify, report, and correct system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates within [*the timeframe(s) outlined within the system's system security plan and as required by CIO 2100.1 and CIO-IT Security-06-30, Managing Enterprise Cybersecurity Risk*] of the release of the updates; and
d. Incorporate flaw remediation into the organizational configuration management process.

SI-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned	

SI-2	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-2 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

13.18.3 SI-2 (2): Flaw Remediation | Automated Flaw Remediation Status

Determine if system components have applicable security-relevant software and firmware updates installed using [*automated mechanisms define in the SSPP*] [*monthly*].

SI-2 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name]	

SI-2 (2)	Control Enhancement Summary Information
☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-2 (2) Describe how the control is implemented.	

13.18.4 SI-2 (3): Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions

(a) Measure the time between flaw identification and flaw remediation; and
(b) Establish the following benchmarks for taking corrective actions: [

(1) BOD Timelines

(a) Within 14 days for vulnerabilities added to CISA's KEV Catalog with a CVE date post FY21.

(b) Per the CISA KEV catalog date or GSA Standard timelines below, whichever is earlier, for vulnerabilities in the CISA KEV catalog with a CVE date in FY21 or earlier.

(c) Within 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.

(2) GSA Standard Timelines

(a) Within 30 days for Critical (Very High) and High vulnerabilities.

(b) Within 90 days for Moderate vulnerabilities.

(c) Within 120 days for Low vulnerabilities for Internet-accessible systems/services.]

SI-2 (3)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

SI-2 (3)	Control Enhancement Summary Information
SI-2 (3) Describe how the control is implemented.	
Part a	
Part b	

13.18.5 SI-3: Malicious Code Protection

a. Implement [*signature based and non-signature based*] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;
b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
c. Configure malicious code protection mechanisms to:
   1. Perform periodic scans of the system [*weekly*] and real-time scans of files from external sources at [*endpoint and network entry/exit points*] as the files are downloaded, opened, or executed in accordance with organizational policy; and
   2. [*Block or quarantine malicious code*]; and send alert to [*administrator, send alert to log*] in response to malicious code detection; and
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

SI-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-3 Describe how the control is implemented.	

SI-3	Control Summary Information
Part a	
Part b	
Part c	
Part d	

13.18.6 SI-4: System Monitoring

a. Monitor the system to detect:

1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [*ensuring the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examining system records to confirm that the system is functioning in an optimal, resilient, and secure state; identifying irregularities or anomalies that are indicators of a system malfunction or compromise*]; and
2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: [*a variety of sources including but not limited to continuous monitoring vulnerability scans, malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers*];

c. Invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the system to collect organization-determined essential information; and
2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide [*the GSA S/SO or Contractor recommended and GSA CISO and AO approved information system monitoring information*] to [*ISSM, ISSO, and System Program Managers who distribute the information to other personnel with system administration, monitoring, and/or security responsibilities*] [*within the timeframe(s) specified in the applicable system security and privacy plan*].

SI-4	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-4 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	
Part e	

SI-4	Control Summary Information
Part f	
Part g	

13.18.7 SI-4 (2): System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis

Employ automated tools and mechanisms to support near real-time analysis of events.

SI-4 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-4 (2) Describe how the control is implemented.	

13.18.8 SI-4 (4): System Monitoring | Inbound and Outbound Communications Traffic

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
(b) Monitor inbound and outbound communications traffic [*continuously*] for [*indicators of compromise (IOCs) including but not limited to known bad IP address(s), URI(s), hash(s) from trusted sources; suspicious DNS activity; large data uploads; and, other unusual or unauthorized activities or conditions as determined by the GSA CISO and AO*].

SI-4 (4)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-4 (4) Describe how the control is implemented.	
Part a	
Part b	

13.18.9 SI-4 (5): System Monitoring | System-Generated Alerts

Alert [*all staff with system administration, monitoring, and/or security responsibilities including but not limited to ISSM, ISSO, System Program Managers, Sys/Net/App Admins, etc.]* when the following system-generated indications of compromise or potential compromise occur: *[compromise indicators may include but shall not be limited to the following:*
- Protected system files or directories have been modified without notification from the appropriate change/configuration management channels.
- System performance indicates resource consumption that is inconsistent with expected operating conditions.
- Auditing functionality has been disabled or modified to reduce audit visibility.
- Audit or log records have been deleted or modified without explanation.
- The system is raising alerts or faults in a manner that indicates the presence of an abnormal condition.
- Resource or service requests are initiated from clients that are outside of the expected client membership set.
- The system reports failed logins or password changes for administrative or key service

accounts.
- Processes and services are running that are outside of the baseline system profile.
- Utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose].

SI-4 (5)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-4 (5) Describe how the control is implemented.	

13.18.10 SI-4 (18): System Monitoring | Analyze Traffic and Covert Exfiltration

Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [*GSA's mail subsystem and internal firewalls between select subnetworks*].

SI-4 (18)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP)	

SI-4 (18)	Control Enhancement Summary Information
☐ System Specific Control	
SI-4 (18) Describe how the control is implemented.	

13.18.11 SI-4 (23): System Monitoring | Host-Based Devices

Implement the following host-based monitoring mechanisms at [*GSA S/SO or Contractor recommended and GSA CISO and AO approved information system components*]: [*GSA S/SO or Contractor recommended and GSA CISO and AO approved host-based monitoring mechanisms*].

SI-4 (23)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-4 (23) Describe how the control is implemented.	

13.18.12 SI-5: Security Alerts, Advisories, and Directives

a. Receive system security alerts, advisories, and directives from [*US-CERT, NIST, OMB, Product Vendors, and Industry Advisors*] on an ongoing basis;
b. Generate internal security alerts, advisories, and directives as deemed necessary;
c. Disseminate security alerts, advisories, and directives to: [*all staff with system administration, monitoring, and/or security responsibilities including but not limited to ISSM, ISSO, System Program Managers, Sys/Net/App Admins, etc.*]; and

d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

SI-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-5 Describe how the control is implemented.	
Part a	
Part b	
Part c	
Part d	

13.18.13 SI-7: Software, Firmware, and Information Integrity

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [*GSA software, firmware, and information*]; and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [*notify the System Owner, ISSO, ISSM, and the GSA Incident Response team.*].

SI-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-6 Describe how the control is implemented.	
Part a	
Part b	

13.18.14 SI-7 (1): Software, Firmware, and Information Integrity | Integrity Checks

Perform an integrity check of [*GSA software, firmware, and information*] [*at startup; at the occurrence of configuration changes or security-relevant events; at least monthly*].

SI-7 (1)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

SI-7 (1)	Control Enhancement Summary Information
SI-7 (1) Describe how the control is implemented.	

13.18.15 SI-7 (7): Software, Firmware, and Information Integrity | Integration of Detection and Response

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [*changes to established configuration settings or unauthorized elevation of information system privileges*].

SI-7 (7)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-7 (7) Describe how the control is implemented.	

13.18.16 SI-8: Spam Protection

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and
b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

SI-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: GSA Enterprise Application Services (EAS) ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-8 Describe how the control is implemented.	
Part a	
Part b	

13.18.17 SI-8 (2): Spam Protection | Automatic Updates

Automatically update spam protection mechanisms [*daily*].

SI-8 (2)	Control Enhancement Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: GSA Enterprise Application Services (EAS) ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	

SI-8 (2)	Control Enhancement Summary Information
SI-8 (2) Describe how the control is implemented.	

13.18.18 SI-10: Information Input Validation

Check the validity of the following information inputs: [*character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content as it relates to:*
(1) Username and password combinations.
(2) Attributes used to validate a password reset request (e.g. security questions).
(3) Personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record).
(4) Biometric data or personal characteristics used to authenticate identity.
(5) Sensitive financial records (e.g. account numbers, access codes).
(6) Content related to internal security functions: private encryption keys, white list or blacklist rules, object permission attributes and settings].

SI-10	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-10 Describe how the control is implemented.	

13.18.19 SI-11: Error Handling

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and
b. Reveal error messages only to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*].

SI-11	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-11 Describe how the control is implemented.	
Part a	
Part b	

13.18.20 SI-12: Information Management and Retention

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

SI-12	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented	

SI-12	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-12 Describe how the control is implemented.	

13.18.21 SI-12 (1): Information Management and Retention | Limit Personally Identifiable Information Elements

Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [*as defined in the SORN*].

Note: Only applicable if PII is stored, processed, or transmitted by the system.

SI-12 (1)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-12 (1) Describe how the control is implemented.	

SI-12 (1)	Control Summary Information

13.18.22 SI-12 (2): Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research

Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [*this policy/process is under development and considers the sensitivity of PII, number of individuals and/or records in the research, testing or training*].

Note: Only applicable if PII is stored, processed, or transmitted by the system.

SI-12 (2)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-12 (2) Describe how the control is implemented.	

13.18.23 SI-12 (3): Information Management and Retention | Information Disposal

Use the following techniques to dispose of, destroy, or erase information following the retention period: [*as defined in CIO-IT Security-06-32, Media Protection*].

Note: Only applicable if PII is stored, processed, or transmitted by the system.

SI-12 (3)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-12 (3) Describe how the control is implemented.	

13.18.24 SI-16: Memory Protection

Implement the following controls to protect the system memory from unauthorized code execution: [*GSA S/SO or Contractor recommended and GSA CISO and AO approved security safeguards*].

SI-16	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-16 Describe how the control is implemented.	

SI-16	Control Summary Information

13.18.25 SI-18: Personally Identifiable Information Quality Operations

a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle [*as part of the PIA review process*]; and
b. Correct or delete inaccurate or outdated personally identifiable information.

Note: Only applicable if PII is stored, processed, or transmitted by the system.

SI-18	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-18 Describe how the control is implemented.	
Part a	
Part b	

13.18.26 SI-18 (4): Personally Identifiable Information Quality Operations | Individual Requests

Correct or delete personally identifiable information upon request by individuals or their designated representatives.

Note: Only applicable if PII is stored, processed, or transmitted by the system.

SI-18 (4)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-18 (4) Describe how the control is implemented.	

13.18.27 SI-19: De-Identification

a. Remove the following elements of personally identifiable information from datasets: [*PII and sensitive PII defined in: https://docs.google.com/spreadsheets/d/1Yb9I9C3qCee8dnkVIIUqIZgrWsA1DoW0xYF2yPjgz0I/edit#gid=1521803081*]; and
b. Evaluate [*as part of the PIA review*] for effectiveness of de-identification.

Note: Only applicable if PII is stored, processed, or transmitted by the system.

SI-19	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control	

SI-19	Control Summary Information
☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SI-19 Describe how the control is implemented.	
Part a	
Part b	

13.19 Supply Chain Risk Management

13.19.1 SR-1: Policy and Procedures

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

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

SR-1	Control Summary Information
Implementation Status: ☒ Implemented ☐ Partially Implemented ☐ Planned	

SR-1	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination: ☒ Inherited from: GSA 2100.1, GSA Information Technology (IT) Security Policy and IT Security Procedural Guide: Information Security Program Plan (ISPP) CIO-IT Security-18-90 ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SR-1 Describe how the control is implemented.	
Part a	1. The GSA supply chain risk management policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for system and information integrity activities. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site. 2. Supply chain risk management procedures are documented in CIO-IT Security-21-117, "IT Security Procedural Guide: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program" and CIO-IT Security-18-90. The procedures facilitate the implementation of the supply chain risk management policy and associated controls. The guides are disseminated GSA-wide via GSA's InSite centralized agency web site.
Part b	Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.
Part c	The GSA OCISO is responsible for reviewing and updating: 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance. 2. CIO-IT Security-21-117 and CIO-IT Security 18-90 every three years and following changes to Federal or GSA policies, requirements, or guidance.

13.19.2 SR-2: Supply Chain Risk Management Plan

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system

services: [*all systems, system components, or system services unless explicitly excluded and approved by the GSA CISO and AO*];

b. Review and update the supply chain risk management plan [*annually*] or as required, to address threat, organizational or environmental changes; and
c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

SR-2	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SR-2 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.19.3 SR-2 (1): Supply Chain Risk Management Plan | Establish SCRM Team

Establish a supply chain risk management team consisting of [*Internal GSA: SCRM Senior Accountable Official and SCRM Executive Board and SCRM Working Group members, as defined in the SCRM Executive Board Charter, External: GSA S/SO or Contractor recommended personnel, roles, and responsibilities as approved by the GSA CISO and AOs*] to lead and support the following SCRM activities: [*Internal GSA: defined in the SCRM Executive Board Charter,*

External: organization-defined supply chain risk management activities.]

SR-2(1)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SR-2(1) Describe how the control is implemented.	

13.19.4 SR-3: Supply Chain Controls and Processes

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [*GSA systems and their components*] in coordination with [*SSO or contractor recommended supply chain personnel as approved by the GSA CISO and AO*];
b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [*SCRM controls (based on FIPS 199 Baseline) identified in the GSA CTW*]; and
c. Document the selected and implemented supply chain processes and controls in [*security and privacy plans; security and privacy plans.*]

SR-3	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

SR-3	Control Summary Information
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SR-3 Describe how the control is implemented.	
Part a	
Part b	
Part c	

13.19.5 SR-5: Acquisition Strategies, Tools, and Methods

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [*Federal: acquisition strategies, contract tools, and procurement methods as defined on the SCRM SAO & Review Board Webpage, Contractor: organization-defined acquisition strategies, contract tools, and procurement methods*].

SR-5	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's	

SR-5	Control Summary Information
Name] SSPP) ☐ System Specific Control	
SR-5 Describe how the control is implemented.	

13.19.6 SR-6: Supplier Assessments and Reviews

Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [*annually*].

SR-6	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SR-6 Describe how the control is implemented.	

13.19.7 SR-8: Notification Agreements

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [*notification of supply chain compromises; results of assessments or audits.*]

SR-8	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SR-8 Describe how the control is implemented.	

13.19.8 SR-10: Inspection of Systems or Components

Inspect the following systems or system components [*as identified by the Supply Chain Risk Management Team as identified in SR-2(1)*] to detect tampering: [*systems or system components as identified by the Supply Chain Risk Management Team as identified in SR-2(1)*].

SR-10	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SR-10 Describe how the control is implemented.	

SR-10	Control Summary Information

13.19.9 SR-11: Component Authenticity

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and
b. Report counterfeit system components to [*the source of the counterfeit component; Federal: GSA SCRM Review Board and as a security incident to the IT Service Desk in accordance with IR-6, Contractor: Contracting Officer.*]

SR-11	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SR-11 Describe how the control is implemented.	
Part a	
Part b	

13.19.10 SR-11 (1): Component Authenticity | Anti-Counterfeit Training

Train [*the SCRM Team as identified in SR-2(1)*] to detect counterfeit system components (including hardware, software, and firmware).

SR-11 (1)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SR-11(1) Describe how the control is implemented.	

13.19.11 SR-11 (2): Component Authenticity | Configuration Control for Component Service and Repair

Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [*all components*].

SR-11 (2)	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SR-11(2) Describe how the control is implemented.	

SR-11 (2)	Control Summary Information

13.19.12 SR-12: Component Disposal

Dispose of [*data, documentation, tools, and system components in accordance with the Media Protection procedural guide or Contractor recommendation as approved by the GSA CISO and AO*] using the following techniques and methods: [*as described in the Media Protection procedural guide or Contractor recommendation as approved by the GSA CISO and AO*].

SR-12	Control Summary Information
Implementation Status: ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination: ☐ Inherited from: [Enter System's Name] ☐ [Source System's Name] Common Control ☐ Hybrid Control (Shared Between [SYSTEMNAME] and [Source System's Name]; see also [Source System's Name] SSPP) ☐ System Specific Control	
SR-12 Describe how the control is implemented.	

Instruction: Appendices vary on a system by system basis. The following appendices are GSA's standard SSPP appendices.
Add any other appendices the System Owner, ISSO, ISSM, or AO deem necessary.

APPENDIX A – Acronyms, Terms and Definitions

Acronym	Full Name
A&A	Assessment and Authorization
AMI	Amazon Machine Image
AO	Authorizing Official
API	Application Programming Interface
BIA	Business Impact Assessment
CCB	Configuration Control Board
CI/CD	Continuous Integration/Continuous Delivery
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CM	Configuration Management
CONOPS	Concept of Operations
COTS	Commercial off-the-shelf
CPO	Chief Privacy Officer
CTW	Control Tailoring Workbook
CUI	Controlled Unclassified Information
EBS	Elastic Block Store
ECR	Elastic Container Registry
ECS	Elastic Container Service
EKS	Elastic Kubernetes Service
ELK	Elastisearch, Logstash, Kibana
ERC	Emergency Response Coordinator
ESS	Enterprise Server Services
FEA	Federal Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GSA	General Services Administration
GUI	Graphical User Interface
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol

Acronym	Full Name
IAM	Identity Access Management
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISP	Internet Service Provider
ISPP	Information Security Program Plan
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MA	Major Application
MFA	Multi-factor Authentication
MOA	Memoranda of Agreement
MOU	Memoranda of Understanding
NACL	Network Access Control List
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OCISO	Office of the Chief Information Security Officer
OMB	Office of Management and Budget
OS	Operating System
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PTA	Privacy Threshold Analysis
PIV	Personal Identity Verification
PM	Program Manager
POC	Point of Contact
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RDS	Relational Database Service
S3	Simple Storage Service
S/SO/R	Services, Staff Offices, Regions
SAOP	Senior Agency Official for Privacy
SCP	Service Control Policy
SDLC	Systems Development Life Cycle
SFTP	Secure File Transfer Protocol
SNS	Simple Notification Service
SORN	System of Records Notice

Acronym	Full Name
SSH	Secure Shell
SSO	Single Sign-On
SSPP	System Security and Privacy Plan
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WAF	Web Application Firewall

TERMS AND DEFINITIONS

Assurance -Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

Audit Log - A chronological record of information system activities, including records of system accesses and operations performed in a given period.

Audit Record - An individual entry in an audit log related to an audited event.

Audit Trail - A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result.

Authentication - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authenticator - The means used to confirm the identity of a user, processor, or device (e.g., user password or token).

Authorization - The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Authorizing Official - A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Availability - Ensuring timely and reliable access to and use of information.

Baseline Configuration - A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

Boundary Protection - Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels).

Boundary Protection Device - A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.

Common Control - A security control that is inheritable by one or more organizational information systems. See Security Control Inheritance.

Compensating Security Controls - The security controls employed in lieu of the recommended controls in the security control baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253 that provide equivalent or comparable protection for an information system or organization.

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control - Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.

Configuration Management - A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Configuration Settings - The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.

Controlled Unclassified Information - A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

Countermeasures - Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system.

Cyber Attack - An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Security - The ability to protect or defend the use of cyberspace from cyber-attacks.

Developer - A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; and (iv) product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.

Hardware - The physical components of an information system.

Hybrid Security Control - A security control that is implemented in an information system in part as a common control and in part as a system-specific control.

Information Security - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Policy - Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information Security Program Plan - Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

Information Security Risk - The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Technology - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Internal Network A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.

Linting - A process by which a linter program analyzes source code in a particular programming language and flags potential problems like syntax errors, deviations from a prescribed coding style, or using constructs known to be unsafe.

Mobile Device - A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.

Network - Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Penetration Testing - A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

Personally Identifiable Information - Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Plan of Action and Milestones - A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Potential Impact - The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS Publication 199 low); (ii) a serious adverse effect (FIPS Publication 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.

Privacy Impact Assessment - An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Threshold Analysis – A document that determines if a privacy impact assessment is required.

Remote Access - Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

Risk - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or

information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Risk Assessment - The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

Risk Management - The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Risk Mitigation - Prioritizing, evaluating, and implementing the appropriate risk reducing controls/countermeasures recommended from the risk management process.

Risk Monitoring - Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.

Risk Response - Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

Safeguards - Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Security - A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Security Assessment Plan - The objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment.

Security Categorization - The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems.

Security Category - The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.

Security Control - A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Security Control Assessment - The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

Security Control Baseline - The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system that provides a starting point for the tailoring process.

Security Control Enhancement - Augmentation of a security control to: (i) build in additional, but related, functionality to the control; (ii) increase the strength of the control; or (iii) add assurance to the control.

Security Control Inheritance - A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.

Security Requirement - A requirement levied on an information system or an organization that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted.

Security Risks - Risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and that considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation.

Software - Computer programs and associated data that may be dynamically written or modified during execution.

System of Records - Notice An official public notice of an organization’s system(s) of records, as required by the Privacy Act of 1974, that identifies: (i) the purpose for the system of records; (ii) the individuals covered by information in the system of records; (iii) the categories of records maintained about individuals; and (iv) the ways in which the information is shared.

System Owner (or Program Manager) - Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

System Security Plan - Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

System-Specific Security Control - A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Assessment - Formal description and evaluation of threat to an information system.

User - Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

Vulnerability - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment - Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

APPENDIX B – References

Applicable Standards and Guidance
The following GSA guidance documents apply to this information system:

- CIO-IT Security-06-30, GSA IT Security Procedural Guide: Managing Enterprise CyberSecurity Risk
- GSA Order ADM 7800.11A, Personal Use of Agency Office Equipment
- GSA Order ADM 9732.1E, Personnel Security and Suitability Program Handbook
- GSA Order CIO 2200.1, GSA Privacy Act Program
- GSA Order CIO 1878.3, Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices
- GSA Order CIO 2100.2C, GSA Wireless Local Area Network (WLAN) Security
- GSA Order CIO 2101.2, GSA Enterprise Information Technology Management (ITM) Policy
- GSA Order CIO 2103.2, Controlled Unclassified Information (CUI) Policy
- GSA Order CIO 2104.1B CHGE 1, GSA Information Technology (IT) General Rules of Behavior
- GSA Order CIO 2110.4, GSA Enterprise Architecture Policy
- GSA Order CIO 2135.2C, GSA Information Technology (IT) Capital Planning and Investment Control (CPIC)
- GSA Order CIO 2140.4, Information Technology (IT) Solutions Life Cycle (SLC) Policy
- GSA Order OSC 2140.2, Management of GSA's Digital Presence
- GSA Order CIO 2160.2B CHGE 3, GSA Electronic Messaging and Related Services
- GSA Order CIO 2231.1, GSA Data Release Policy
- GSA Order CIO 9297.2C CHGE 1, GSA Information Breach Notification Policy
- GSA Order CIO P 2165.2 CHGE 1, GSA Telecommunications Policy
- GSA Order CIO 2180.2, GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
- GSA Order ADM 2181.1, Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors
- GSA Order CIO P 2182.2, Mandatory Use of Personal Identity Verification (PIV) Credentials
- GSA Order CIO 1820.2, GSA Records Management Program
- GSA Order OSC 2106.2, GSA Social Media Policy

Note: All GSA Policies and Procedural Guides can be found at the following URL.

Applicable Federal Laws
The following Federal Laws apply to this information system:

- Public Law 113-283, Federal Information Security Modernization Act (FISMA) of 2014
- Clinger-Cohen Act of 1996, also known as the Information Technology Management Reform Act of 1996.
- Federal Financial Management Improvement Act of 1996 (FFMIA), OMB Implementation Guidance for the FFMIA.
- 5 U.S.C. § 552a, Privacy Act of 1974
- HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection
- HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors
- OMB Circular A-130 Management of Federal Information Resources
- OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy
- OMB M-17-15, Recission of Memoranda Relating to Identity Management
- OMB 21-07, Completing the Transition to Internet Protocol Version 6 (IPv6)
- U.S. Code 278g-3, Computer Standards Program

Applicable NIST Publications

The following NIST publications apply to this information system:

- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-60 Volume I, Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-60 Volume II, Revision 1: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-63-3, Digital Identity Guidelines
- NIST 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems
- NIST SP-800-39, Managing Information Security Risk

Note: NIST Computer Security Publications series can be found at the following URLs:

NIST SP Series

NIST FIPS Series

APPENDIX C – Hosted Subsystems (if applicable)

Subsystem Name	Subsystem Purpose/Description	Program Manager/ System Owner

Instruction: Attachments vary on a system by system basis. The following appendices are GSA's standard SSPP attachments.

Attachments

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(s) (if applicable)

Attachment 5: Control Tailoring Workbook (CTW)

Attachment 6: Control Summary Table (based on FIPS 199 Categorization)

Attachment 7: Contingency Plan (with Business Impact Assessment)

Attachment 8: Contingency Plan Test Report

Attachment 9: Incident Response Plan

Attachment 10: Incident Response Plan Test Report

Attachment 11: Configuration Management Plan (FIPS 199 Moderate and High only)

Attachment 12: Continuous Monitoring Plan (if applicable)

Attachment 13: Rules of Behavior (if applicable)

Attachment 14: Code Review Report (if applicable)

Instruction: Attach any additional documents the System Owner, ISSO, ISSM, or AO deem necessary to understand the security implementation of the system.