IT Security Procedural Guide: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations Process CIO-IT Security-21-112

Revision 1

January 5, 2026

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – May 27, 2022		
N/A	Palmer, Hoyt, Turnau, Berlas	New guide created for protecting CUI in Nonfederal systems	Provide guidance for implementing security requirements from NIST SP 800-171, 800-172, and selected privacy controls from 800-53, Revision 5.	N/A
		Revision 1 – January 5, 2026		
1	Normand/ Klemens/ Peralta	Revisions include: • Updated to NIST SP 800-171r3, and 800-172r3 (Draft). • Moved references to an Appendix. • Revised Appendix C to contain only Showstopper requirements.	Align to the latest NIST and GSA guidance.	Throughout

Approval

IT Security Procedural Guide: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations Process, CIO-IT Security 21-112, Revision 1, is hereby approved for distribution.

DocuSigned by:
Joseph Hoyt
CA8EF810EDA7425...

Joseph Hoyt
Acting GSA Chief Information Security Officer

DocuSigned by:
Richard Speidel
171D5411183F40A...

Richard Speidel
GSA Chief Privacy Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP), at ispcompliance@gsa.gov regarding security requirements and the guide, and privacy.office@gsa.gov regarding privacy controls.

Table of Contents

List of Tables and Figures

Note: Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Appendix A or Appendix B.

1 Introduction

To comply with Federal standards, nonfederal systems and organizations shall implement the specific security requirements[1] from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171r3, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," for protecting the confidentiality of Controlled Unclassified Information (CUI); selected requirements from NIST SP 800-172r3 (Draft), "Enhanced Security Requirements for Protecting Controlled Unclassified Information"; and, selected Privacy requirements from NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations."

The security requirements in NIST SP 800-171 and 800-172 have been tailored for nonfederal entities by eliminating requirements, controls, or parts of controls that are:

- uniquely Federal;
- not directly related to protecting the confidentiality of CUI; or
- expected to be routinely satisfied by nonfederal organizations without specification.

NIST SP 800-171 and NIST SP 800-172 security requirements are derived from Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems," and security controls from NIST SP 800-53 and are based on 32 Code of Federal Regulations (CFR) Part 2002, "Controlled Unclassified Information." Information about CUI and CUI Categories is available at the National Archives and Records Administration (NARA) CUI webpage and the General Services Administration (GSA) CUI Program webpage.

1.1 Purpose

This procedural guide defines the processes and procedures that will be used to ensure that nonfederal systems protect CUI in accordance with NIST and GSA requirements. It identifies the processes, steps, and activities to be followed to determine the applicability of using this process and verifying CUI is appropriately protected. This guide assists agency and vendor personnel in understanding the process and their responsibilities throughout the process.

The protection and marking of CUI serves the purpose of limiting access to CUI which includes not only Federal information but also personally identifiable information (PII), financial and contractual information potentially including proprietary information contained therein. For example, many of the documents developed during the processes described in this guide are marked CUI and require special handling such as encrypting the documents with Federal Information Processing Standard (FIPS) validated encryption when sent via email.

1.2 Scope

As stated in NIST SP 800-171, its requirements are applicable under the following conditions:

- CUI is resident in a nonfederal system and organization;

[1] The term requirements in this guide will be used to refer to requirements from NIST SP 800-171 and 800-172, more generally to requirements from other Federal mandates or policies. The term controls will be used when referring to controls from NIST SP 800-53 and controls (i.e., features or mechanisms) systems have been implemented to meet requirements.

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

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

Usage of this process shall be coordinated with the GSA Office of the Chief Information Security Officer (OCISO) and requires GSA Chief Information Security Officer (CISO) approval. Upon approval, the related IT Security and Privacy Requirements identified in GSA IT Security Procedural Guide 09-48, "Security and Privacy Requirements for IT Acquisition Efforts" for nonfederal systems and organizations are required to be included in contract solicitation documents.

1.3 References

Appendix A provides links to references used throughout this guide.

2 Process for Protecting CUI in Nonfederal Systems and Organizations

The process steps for protecting CUI in nonfederal systems and organizations have been derived from the NIST Risk Management Framework (RMF) phases. GSA has tailored and condensed the NIST RMF into five phases for this guide:

- Phase 1 - Prepare
- Phase 2 - Document
- Phase 3 - Assess
- Phase 4 - Authorize
- Phase 5 - Monitor

The key activities within each phase are described in the ensuing sections. Links to documents, templates, job aids, and checklists required as part of the phases are provided in Appendix B. Throughout the remainder of this guide deliverables will be referred to by their respective titles with a reference and link to Appendix B when appropriate.

2.1 Phase 1 – Prepare

Phase 1 - Prepare is made up of three sub-phases as listed in Table 2-1 and described in the following subsections. Table 2-1 includes the activities, deliverables, or job aids, and who is responsible in each phase.

[2] Nonfederal organizations that collect or maintain information on behalf of a federal agency or that use or operate a system on behalf of an agency must comply with the requirements in Federal Information Security Modernization Act (FISMA).

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

Table 2-1. Deliverables/Job Aids and Activities in Phase 1

Sub-Phase	Deliverables/Job Aids*	Activity	Responsibility
1	**Deliverable** - FIPS-199 Security Categorization Template (Deliverable)	Identify and verify information types stored, processed, or transmitted.	Vendor
1	**Deliverable** – Federal Risk and Authorization Management Program (FedRAMP) versus 800-171 Qualifying Template (Optional)	Determine authorization path.	Vendor (Optional)
2	**Job Aid** - GSA Nonfederal Security and Privacy Kickoff Slides (Job Aid)	Schedule and hold GSA Nonfederal Security and Privacy Kickoff Meeting	GSA
2	**Job Aid** - Project Work Breakdown Structure (WBS) (Optional)	Part of Kickoff Meeting (Optional)	GSA and Vendor (Optional)

*Links to templates/documents are provided in Appendix B.

2.1.1 Identify and Verify Information Types/Determine Authorization Path

In the first sub-phase the vendor completes:

- The FIPS 199 security categorization template to determine the types of information, stored, processed, or transmitted by the nonfederal information system. Only nonfederal systems with a FIPS 199 confidentiality level of Moderate (based on CUI being in-scope) follow the process described in this guide. NIST SP 800-60 Volumes I and II are used to identify the information types handled by the system. The FIPS 199 security categorization process is completed by the vendor, in collaboration with the GSA Information System Security Officer (ISSO) and Information System Security Manager (ISSM). It is then approved by the GSA data owner, the CISO, and the Senior Agency Official for Privacy (SAOP)–for systems with PII, or their designated representatives. Designated representatives must be Federal employees. Approval may occur by using GSA's template or collaborating within GSA's Government, Risk and Compliance (GRC) tool.
- OPTIONAL - The FedRAMP versus 800-171 Qualifying Template may be used to determine the applicability of using the process described in this guide. Answering the questions in the template can lead to a determination on whether the system qualifies to continue following the process in this guide or pursue a FedRAMP authorization based on system design and cloud applicability. In order to continue following the process in this guide the GSA OCISO will coordinate with the vendor and request GSA CISO approval. Upon GSA CISO approval to use the process in this guide GSA will arrange the NIST 800-171 Engagement Kick-Off Meeting described in the following section.

2.1.2 NIST 800-171 Engagement Kick-Off Meeting

In the second sub-phase, vendors participate in a kick-off meeting with the GSA to review the process for protecting CUI in nonfederal systems; review required deliverables and expected timelines; describe showstoppers that will preclude approval; discuss general responsibilities and the overall quality expectations for deliverables.

During the kick-off meeting, GSA will provide the vendor all necessary GSA templates and job aid documents. GSA will provide the vendor with an overview of the 800-171 process including approval checkpoints. GSA and vendors will introduce points of contact (POCs) and discuss expectations.

Optionally, GSA's WBS template may be provided for use. This WBS may be used to track the key deliverables, GSA reviews, GSA approvals, and the overall project schedule.

2.1.3 Determine Vendor Solution Readiness

In sub-phase 2.1.3, the vendor will represent its solutions architecture to the GSA. The vendor solutions architecture and critical capability briefing is for the vendor to provide a technical overview of their solution offering detailing their boundary scope, system architecture, critical security capabilities, and identify any known security and privacy requirement gaps associated with the requirements identified in Appendix C: Showstopper Security and Privacy Requirements for the Nonfederal Security Approval Process. Vendors are recommended to closely align this deliverable to the CUI Nonfederal Security Architecture Review Checklist required as a deliverable in section Phase 2 - Document as GSA will be utilizing the vendor completed checklist to determine the overall readiness of the vendor solution for Phase 3 - Assess. Table 2-2 details GSA's Architecture Critical Security Capabilities.

Table 2-2. Architecture Critical Security Capabilities

Critical Security Capabilities	Requirement
Access Control	The vendor must have a mature process in place for authorizing, provisioning, managing, and monitoring accounts. The System Security and Privacy Plan (SSPP) control implementation statements must clearly describe the technical mechanisms that are in place to control the flow of information within the system. (Identity and Access Management [IAM], Active Directory, Federation, Local Accounts) **Note** This discussion should include mechanisms for ALL areas of the infrastructure stack.
Multi Factor Authentication	Discuss the multifactor authentication (MFA) methods, technologies, and pin sending methods for ALL vendor personnel and Federal user and privileged user access (as applicable).
Configuration Management	Discuss how configuration baselines are established. They should be derived from industry sources such as Center for Internet Security (CIS), vendor recommendations, and other industry best practices. Describe the automated processes/technologies in place to manage and control configuration changes.
Vulnerability Management	Vulnerability scanning shall be fully authenticated, tools updated with the most recent vulnerability definitions, and all non-invasive plugins enabled for operating system (OS)/Database (DB)/Container/Web scans (as applicable). If container technologies are in use, identify the tool(s) used for vulnerability management. **Note** Please align this discussion with Appendix G: Scanning Guidance and Appendix H: Container Guidance. Scan tools shall have the ability to produce reports aligning to the Common Vulnerability Scoring System (CVSS) scoring. Vulnerabilities shall be remediated following best practice time frames. (Critical (Internet facing) = 15 Days; Critical/High = 30 Days; Moderate = 90 Days, Low = 180 days)

Critical Security Capabilities	Requirement
Administrative Access	Provide an overview of how system administrators access the environment. This should be inclusive of all hops and authentication points administrators must go through including but not limited to Virtual Private Network (VPN), jump/bastion hosts, SecureShell (SSH)/Remote Desktop Protocol (RDP) access to managed assets. **Note** Please align this discussion with the GSA Secure Admin Access Guidance in Appendix F: Remote Access Guidance.
System and Communications Protections	Describe how/where data is encrypted in transit and at rest. Include protocols, modules, and ciphers being used along with their strength. Describe the boundary protection mechanisms in place. Cover both ingress and egress. Describe how internal and external data flows are encrypted.
Security Tools	List all security management tools that support the infrastructure to include at a minimum, security information and event management (SIEM) tool, vulnerability scanners (OS, DB, Web, Container [if applicable]), firewalls, intrusion detection system (IDS)/intrusion prevention system (IPS), antivirus/malware, configuration management.
End of Life and Obsolete Technology	Confirm all software; security protocols; and security encryption ciphers that are either no longer supported or deprecated are not present in the environment. Outdated/Unsupported software is defined as software that is End of Life (EOL) and no longer supported by the vendor. Outdated encryption protocols are anything below Transport Layer Security (TLS) 1.2. Outdated encryption is any encryption that utilizes known weak or vulnerable ciphers.
External and Leveraged Services	If corporate shared services or external Software-as-a-Service (SaaS) integrations are used, they must be appropriately defined and documented within the system boundary. GSA will evaluate each integration on a case-by-case basis utilizing the information provided in the external services tab of the systems inventory. If the system is built on a FedRAMP authorized Infrastructure-as-a-Service (IaaS) provider, the services in use must also be FedRAMP authorized. GSA will evaluate each non-FedRAMP authorized IaaS service for use on a case-by-case basis.

Additionally, vendors are encouraged to perform a self-assessment against the security and privacy requirements in Appendix C of this guide to identify any known gaps and detail them in the Architecture and Critical Capability Briefing. Vendors are required to especially focus on requirements identified as showstoppers depicted in Appendix C of this guide and summarized below:

- Access Control - 03.01.02, 03.01.12
- Identification and Authentication - 03.05.03
- Risk Assessment - 03.11.02
- System and Communications Protection - 03.13.01, 03.13.08, 03.13.11
- System and Information Integrity - 03.14.01
- System and Services Acquisition - 03.16.02

The GSA security team (i.e., ISSO, ISSM, CISO) will provide feedback related to potential areas of concern that may prevent successful completion of the CUI Nonfederal review process.

2.2 Phase 2 - Document

During this phase, the system's security and privacy requirements must be documented by the vendor in sufficient detail using the GSA provided CUI Nonfederal SSPP Template. Privacy requirements are required for systems with a Privacy Impact Assessment (PIA). The SSPP describes how the security and privacy requirements are implemented, partially implemented, or planned to be implemented for all assets/devices in scope of the information system boundary as identified in the system architecture diagram and system inventory. Security and privacy requirements that are other than fully implemented (i.e., partially implemented or planned) require a statement detailing vendor planned actions to fully address the requirement.

Table 2-3 includes the deliverables/job aids and activities/guidance and who is responsible in this phase.

Table 2-3. Deliverables/Job Aids and Activities/Guidance in Phase 2

Deliverables/Job Aids*	Activity/Guidance	Responsibility
Deliverable - CUI Nonfederal SSPP Template	Document system characteristics and implementations to satisfy security and privacy requirements.	Vendor
Deliverable - Integrated Inventory, Leveraged and External Services Workbook Template (attachment to SSPP)	Identify system assets, Uniform Resource Locators (URLs), and services.	Vendor
Deliverable - Privacy Threshold Assessment (PTA) (attachment to SSPP)	Document if PII is in scope, if so, a PIA is necessary.	Vendor
Deliverable - PIA - Conditional Based on PTA Outcome (attachment to SSPP)	Document how and when PII is collected, stored, shared, and managed.	Vendor
Deliverable - CUI Nonfederal System Security Architecture Review Checklist (attachment to SSPP)	Identify if the system architecture and vendor processes are clearly defined and address the security and privacy requirements.	Vendor
Deliverable - Supply Chain Risk Management Plan (attachment to the SSPP)	Document how the vendor manages supply chain risk.	Vendor
Job Aid - See Appendix C	Lists the Showstopper requirements from NIST SP 800-171 and 800-172.	GSA provides
Job Aid - See Appendix D	Guidance material for properly documenting the system boundary.	GSA provides
Job Aid - See Appendix E	Guidance material for writing security and privacy requirements.	GSA provides
Job Aid - See Appendix E	Guidance on secure remote access to nonfederal systems processing CUI.	GSA provides
Job Aid - See Appendix G	Guidance on scanning nonfederal systems processing CUI.	GSA provides

*Links to templates/documents are provided in Appendix B.

2.2.1 PTA and PIA Approval

A PTA is required. PIA is conditionally required depending on the responses provided within the PTA. The completed PTA, and PIA if applicable, must be reviewed and approved by the GSA security team and GSA Chief Privacy Officer (CPO). Completed PTAs and PIAs (if applicable) are submitted to the ISSO, ISSM, Contracting Officer (CO) or Contracting Officer Representative (COR), and the GSA Privacy Officer at privacy.office@gsa.gov. Review and approval may occur by using GSA's template or collaborating within GSA's GRC tool.

2.2.2 Architecture and Initial SSPP Submission and Approval

This initial SSPP submission focuses on achieving mutual agreement on the system boundary, architecture, and inventory of the vendor's solutions offering; attaining an understanding of the implementation approach and status for critical showstopper security and privacy requirements; and, achieving general consensus on the detail and quality for all other requirements.

Vendors are asked to first complete sections 1 and 2 of the SSPP template (see Appendix B) and the security and privacy requirements identified as showstoppers in Appendix C of this guide and summarized below:

- Access Control - 03.01.02, 03.01.12
- Identification and Authentication - 03.05.03
- Risk Assessment - 03.11.02
- System and Communications Protection - 03.13.01, 03.13.08, 03.13.11
- System and Information Integrity - 03.14.01
- System and Services Acquisition - 03.16.02

Additionally, the vendor must provide the required SSPP attachments identified in Table 2-3 and Architecture Review Checklist with showstopper security and privacy requirements addressed.

The guidance identified in Appendices D, E, and F of this document and Section 2.2.2.1 below should be used as guidance to inform vendor SSPP security and privacy requirement implementations. This guidance describes areas of specific discussion and sets expectations on the quality and completeness of security and privacy requirement narratives in the SSPP.

Following vendor submission of the required deliverables in this phase as identified in Table 2-3, the GSA security team will perform its reviews to ensure completeness and accuracy providing feedback to the vendor should updates be required.

Documents that are satisfactorily updated and accepted by the GSA security team will be formally presented (via summary briefing) to the GSA CISO for concurrence. GSA CISO approval of the vendor's initial SSPP and security architecture is required before commencing to full documentation of all other security and privacy requirements.

2.2.2.1 Architecture and Initial SSPP Submission and Approval Guidance and Requirements:

The information system is described throughout Sections 1 and 2 of the GSA Nonfederal System SSPP template. The first section includes general information about the system (e.g., system name, owner, security personnel, types of users) and a description of the system's

purpose. A key subsection of Section 1 of the SSPP is the FIPS categorization of the system (see Section 2.1.1).

Section 2 of the SSPP provides detailed information about the system and its environment of operation. The level of detail provided in the SSPP should be commensurate with the security categorization of the information system. Specific guidance for Section 2 of the SSPP is provided below.

Guidance for SSPP Section 2.0 – System Environment

This section is fundamental. It defines the overall system boundary on which everything else is based including security and privacy requirements discussions. As per the GSA Nonfederal System SSPP template, the section requires a detailed architecture, inventory, data flows, and ports, protocols, and services for the system. The architecture must be inclusive of everything in the related system boundary with related access and connection flows across all internal boundary enforcement points (i.e., Virtual Local Area Networks [VLANs], Firewalls, etc.) within the system boundary and external flows to:

- the Internet
- external systems
- IaaS/SaaS/Platform-as-a-Service (PaaS) integrations
- the corporate network (as applicable)

The information system must include details at the port, protocol, services level, and identify direction (inbound, outbound, or both) for related access/authentication flows for all user groups including vendor and customer user level and privileged level access. An approved architecture and SSPP including critical security and privacy requirements is necessary to further the process. If the SSPP and architecture cannot be approved, continued progress is not possible. Review Appendix D: Boundary Diagram Guidance and FedRAMP Approval Boundary Guidance document for detailed boundary scope guidance. While the FedRAMP document is specific to the FedRAMP program, the general principles are universally applicable.

Below are key architecture and boundary scope review conditions GSA will be looking for. Please heed the guidance in the ensuing tables in forming your architecture and related discussion points in this section. Additional detail can be found in Appendix D: Boundary Diagram Guidance.

Table 2-4. Architecture Critical Security Capabilities

#	Architecture Diagram Checklist Item
1	The diagram must include a predominant border drawn around all system components and services included in the system boundary. Include separate borders around protected enclaves, subnets, and demilitarized zones (DMZs); and external connections such as leveraged SaaS, third party connections to other vendors, and/or the corporate network.
2	The diagram(s) and narratives should include ALL assets, services, devices, and software, both physical and virtual, which constitute the information system. The diagram should include Continuity of Operations/Disaster Recovery (COOP/DR) site integrations as well as any test/development environments that are in the boundary.

#	Architecture Diagram Checklist Item
3	The system boundary contains all components, devices, services, communication paths (virtual private networks [VPNs], application programming interface [API] calls, etc.). Integration points and network interconnections with external systems, networks, VPNs, APIs, and services must be well-defined in the architecture and securely implemented. Diagram(s) should be sufficiently detailed and identify flows with source/destination, ports/protocols, and whether the related traffic is encrypted or not. References to ports/protocols table(s) are acceptable (for large sets of ports).
4	All access control mechanisms, such as firewalls, router access control lists (ACLs), subnets, proxies, and cloud-based analogs such as firewalls and network access controls shall be fully documented in the architecture diagram and supporting discussion. A ports, protocols, and services table should be included and describe at a high level all communication flows at the ingress/egress boundary, administration, and all internal all external boundary enforcement points. The table should include: • Direction (Inbound, Outbound, or Both) • Boundary Crossing (Y/N) • Source Internet Protocol (IP) Domain Name System (DNS) Name or Resource Type • Destination IP or DNS Name or Resource Type • Ports (T or U) i.e., tcp/443 • Services • Purpose • Encrypted (Y/N) • Data Sensitivity
5	Leveraged IaaS and PaaS services shall be depicted in the boundary and documented in the CUI Nonfederal System Inventory, Leveraged and External Services Workbook Template. All leveraged IaaS or PaaS that support delivery of the system shall be either FedRAMP authorized or approved by the GSA on a risk-basis.
6	The vendor must complete the Inventory: External Services tab of the Integrated Inventory, Leveraged and External Services Workbook in Appendix B. The External Services tab of the workbook is used to identify all external integrations (e.g., SaaS services, connections to corporate networks, etc.) to determine if it can be used with a supporting basis for approval (e.g., FedRAMP authorized, GSA risk approved, included in system boundary, or not approved). In general, this review includes details on the data type (government/non-government, sensitivity), nature of connection and type of use (inbound, outbound, or both), encryption, authentication, and additional details. If external non-FedRAMP authorized cloud services are in use, create a subsection under Section 2.0 titled 'Third-party SaaS Solutions and Corporate Shared Service Integrations.' Below is a sample intro statement for this section. <Vendor> leverages the following third-party SaaS solutions to improve user and operational security. <Vendor> has documented several security considerations including flow direction, authentication, MFA, encryption, and data contents regarding these external SaaS solutions. The SaaS integrations have been approved for use by the GSA CISO. **Note** Third-party SaaS solutions will be considered on a risk basis with preference for solutions identified as FedRAMP authorized in the FedRAMP Marketplace; all other SaaS will be considered on a risk-basis.
7	Ensure all authentication points (this includes but is not limited to Cloud consoles, jump hosts, machine resources, application, API, enablers, etc. [as applicable]) in the architecture diagram are described in the supporting discussion. All authentications shall be with MFA including for all privileged and non-privileged users; and Internet accessible logins within this system.

#	Architecture Diagram Checklist Item
8	Technology from prohibited vendors shall not be used. Per Section 1634 of Public Law 115-91 and 52.204-25 of the Federal Acquisition Regulation (FAR), these companies (at this time) include Kaspersky Lab, Huawei, ZTE, Hikvision, Hytera, and Dahua and their subsidiaries and affiliates.

Table 2-5. Data Flow and Routing Paths

#	Data Flow and Routing Paths Checklist Item
1	Section 2 of the SSPP shall document all data flows in both narrative and diagram forms. Multiple diagrams may be used; this is recommended. Diagram(s) in this section should be sufficiently detailed and identify flows to all components and support services with source/destination, ports/protocols, or whether the related traffic is encrypted or not. If not encrypted, there needs to be a description of the data contents, sensitivity, if the data is Government data, and which users have access to the data.
2	Data flow through approved external or internal Continuous Integration (CI) and Continuous Deployment (CD) systems and code repositories shall be documented in narrative and diagram versions in the SSPP.

Table 2-6. Key Technical Security Considerations

#	Data Flow and Routing Paths Checklist Item
1	All systems shall utilize MFA for both privileged and non-privileged user authentication. Further, systems leveraging certificate-based authentication shall not be downgraded to only username and password authentication. MFA methods used will be evaluated by the GSA security team to ensure alignment with NIST SP 800-171.
2	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 should be reposed in a manner that ensures BCP, DR plans, and COOP are consistent with NIST requirements.
3	Authenticators (e.g., passwords), PII and payment card industry (PCI) data are required to be encrypted 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. Encryption ciphers shall be FIPS-approved and modules FIPS 140-2 validated with module certificate numbers provided.
4	A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems. GSA will consider the risk to CUI data if the vendor fails to comply with Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directives (BOD) and Emergency Directives (EDs) as identified on the CISA Cybersecurity Directives web page. Further, CISA Known Exploited Vulnerabilities (KEV) are available at the following link: Known Exploited Vulnerabilities Catalog | CISA. GSA considers residual CISA KEV vulnerabilities that cannot be corrected as a Showstopper condition.
5	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.
6	Unsupported System Components: The continued usage of EOL Software requires a risk evaluation to be performed by the GSA security team. GSA considers residual EOL software vulnerabilities that cannot be corrected as a Showstopper condition.

2.2.3 Complete SSPP Submission and Approval

After Architecture and Initial SSPP Submission and Approval, the vendor is to complete and submit the remainder of the SSPP and Architecture Checklist to GSA for review to determine if the plan is complete, consistent, and satisfies the security and privacy requirements for the information system. The GSA security team will review and provide feedback to the vendor should updates be required.

Documents that are satisfactorily updated and accepted by the GSA security team will be formally presented (via summary briefing) to the GSA CISO for concurrence. GSA CISO approval of the vendor's complete SSPP and security architecture is required before commencing into the assessment. The GSA security team MUST approve the SSPP before proceeding to assessment. If the vendor proceeds with assessment before SSPP and architecture approval and without a signed Security Assessment Plan (SAP) (see Section 2.3.2), it is at risk of having to reassess the environment and therefore prolonging the overall engagement.

A Supply Chain Risk Management (SCRM) Plan must be included as an attachment to the SSPP. It may be a vendor's existing plan that is consistent with NIST SP 800-161 or documented in a template provided by GSA.

2.2.3.1 Documentation of Requirement Implementations

The vendors completed SSPP inclusive of all security and privacy requirements as listed in Appendix C documented using the GSA provided SSPP template will be reviewed to 1) ensure the requirements are sufficiently detailed and 2) encompass all asset and device components included in the information system boundary. The GSA security team will use the ensuing guidelines in our review. It is highly recommended vendors heed these guidelines in their documentation preparation to ensure expectations for level of detail and quality are aligned.

Guidance for section 3 of the SSPP Requirements

The requirement implementation statements must be clear, concise, consistent, and complete; and describe the who, what, when, where, and how the requirement is implemented. It is not sufficient to simply restate the requirement; statements must specifically describe the vendor's implementation to allow a detailed understanding of protection mechanisms supporting the requirement(s). Additional writing guidance can be found in Appendix E: Writing Security and Privacy Requirements Guidance and Table 2-7.

Table 2-7. Security and Privacy Requirements Discussion Statements

#	Security and Privacy Requirements Discussion Statements Checklist Item
1	Reference the discussion in NIST SP 800-171, 800-172, and 800-53 in forming your response to the security or privacy requirement. The discussion provides additional information to facilitate the implementation and assessment of the requirements. The discussion section associated with each CUI requirement is informative, not normative. It is not intended to extend the scope of a requirement. Additionally, 800-171A, 800-172A, and SP 800-53A may be referenced to inform vendors' implementation statements for security and privacy requirements.
2	If the security or privacy requirement status is "Partially Implemented" or "Planned to be Implemented," enter a description of the planned action in the bottom of the implementation statement. Additionally, if a finding remains as an open item in the POA&M, the security requirement must be changed in the SSPP to "Partially Implemented" or "Planned to be Implemented." The bottom of the implementation statement must have the POA&M ID in bold letters, and the recommendation statement from the independent SAR, when completed. See below for an example. **3.1.8 Limit unsuccessful logon attempts.** ☐ Implemented ☒ Partially Implemented☐ Planned to be Implemented ☐ Not Applicable **ACME Infrastructure Accounts** Authentication and DUO two-factor is required to access ACME information system resources. The password requirements include: ● Lockout after 10 invalid login attempts for a 30 minute duration period. **ACME Central Portal Application (Customer Accounts) -** The ACME Central Portal is by default configured to limit attempts to login. Customers must wait 15 minutes to login to their account after 24 login attempts within 30 minutes. Captcha is also used for suspicious login attempts. An email is sent to the customer if a suspicious login is detected. **ACME Planned Action Statement:** Requirement 3.1.8 - Unsuccessful logon attempts are limited to 10 failed attempts within 30 minutes in all systems in the ACME portal which are set to 24 failed attempts within the same time period. Limit unsuccessful logon attempts to 10 failed attempts within 30 minutes consistent with policy. POA&M ID Reference: ACME-A-2022-0001.
3	Inheriting a security requirement, in part or in full, from another source, should not be marked as "Not Applicable." Mark the implementation as appropriate. Documentation should be available to verify any claims of inheritance. Reflect the inherited portion of the requirement under its own section heading. Repeat for the Vendor portion. See below for example.

#	Security and Privacy Requirements Discussion Statements Checklist Item
4	If the security and privacy requirement status is "Not Applicable," a clear description of the justification and itemization of any evidentiary artifacts supporting the position must be provided in the SSPP. **Note** A requirement that is specifically not being implemented due to operational requirements does not make it not applicable. **3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.** ☒ Implemented ☐ Partially Implemented☐ Planned to be Implemented ☐ Not Applicable **INHERITED PORTION OF THE REQUIREMENT** **Primary and Secondary Datacenter** ACME contracts with EXAMPLE, a global commercial data center provider for both the Primary and Secondary Datacenter that provides hosting services for ACME for in-scope information systems. EXAMPLE undergoes independent assessments and physical access controls are reported through SOC 2 Type 2 reports. ACME receives copies of the EXAMPLE's SOC 2 Type 2 assessment report, reviews it, and retains it on file. Physical access authorizations are enforced at the Primary and Secondary Datacenters as follows: ● Verifying individual access authorizations before granting access to the facility; and ● Controlling ingress/egress to the facility using the following physical access control systems: ○ Security checkpoint badging process including security guard review and verification of government issued identification prior to authorizing entry into the controlled datacenter. After identification verification, the individual receives a badge; ○ After the security checkpoint, the badge opens a two-door mantrap; ○ A retina scan (which is setup during the first visit to the datacenter) releases the mantrap and provides entrance to the datacenter where a locked cage protects the ACME system; and ○ A cage combination provides access to the ACME system. The cage combination was set up when the contract between EXAMPLE and ACME was established. Monitoring of physical facilities and support infrastructure for in-scope information systems is inherited from the EXAMPLE Primary Datacenter. EXAMPLE monitors physical access to detect and respond to physical security incidents. The datacenter is monitored and recorded using closed circuit cameras which are managed 24x7, 365 days per year, by EXAMPLE security officers and the EXAMPLE network operations center. **ACME IMPLEMENTATION STATEMENT** The ACME cage in the EXAMPLE Datacenter is equipped with alarms that feed into ACME's Enterprise Security Operations Center (SOC) to monitor component usage, temperature and humidity level, and overall system and security logging. Incidents, if any, follow ACME Incident Reporting and Escalation Procedures and are reported to the ACME Security Team. Only authorized ACME personnel have access to perform maintenance on in-scope systems. The ACME Security Manager develops, approves, and maintains a list of individuals with authorized access to the ACME Primary and Secondary Datacenter cages where the in-scope information system resides.

#	Security and Privacy Requirements Discussion Statements Checklist Item
5	Ensure all technologies referenced or addressed in Section 3 Security and Privacy Requirements discussions are detailed in Section 2.0 in the architecture and related inventory (Hardware, Software, URL, Leveraged IaaS, and External Services) as applicable.
6	Security and/or privacy requirements that require a customer action to fully implement, require a Customer Responsibility Statement. Identify any security requirements having agency customer responsibilities to ensure CUI data is secure in the vendor's solution. Information must be provided on how the customer will comply with a security requirement for any area (e.g., management or metering portal, etc.) of the system that is provided by the vendor but where customer agencies have implementation responsibility. For example, the vendor may provide an interface for the customer to manage data connectors and API keys. This interface will provide authentication of the customer administrators to perform duties on the vendor's solution. For the customer to comply, the vendor must provide guidance about how the customer configures the vendor's system to provide MFA. Vendors may choose to provide the MFA method (e.g., tokens, etc.), provide the means (e.g., accept SAML 2.0 assertions), or both. Areas such as this where both the vendor and the customer have responsibility for implementing the requirement are referred to as "Shared Responsibilities" Where there are customer responsibilities, include detailed customer responsibilities for those security requirements by creating a new subsection under the security requirement implementation statement titled "Customer Responsibility." In this new section, identify the customer's responsibility relating to the shared touch point for everything the customer must either configure or provide. **3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.** ☒ Implemented ☐ Partially Implemented☐ Planned to be Implemented ☐ Not Applicable **(Privileged) AWS Console and AWS Services:** The AWS user roles are considered privileged and comprise DevOps, VisualOps (read-only), and InfoSec. AWS MFA for privileged IAM users of the AWS Management Console, Shield Advanced, Macie, GuardDuty, Inspector and AWS Systems Manager is implemented using mobile device authenticator apps supporting TOTP. MFA is required for all AWS IAM accounts. **(Privileged) MFA to VPC SSM Session Manager to EC2:** Dedicated SSM Session Managers are deployed to each in-scope VPC and only allow connectivity from the ACME corp network. Users connect to the corporate network via MFA with Okta. Users then connect to the SSM via UN/PW with Authy Token. Privileged users access EC2 endpoints via SSH 2.0 with separate authentication to the machine ssh forwarding thru the SSM host as a bastion. **(Privileged) Third Party Cloud SaaS Integrations:** ACME Portal uses Stark industries SaaS for performance alerting and monitoring. All User connectivity to Stark SaaS requires UN/PW + TOTP Authentication. The system transmits telemetry data to Stark SaaS with token based authentication over HTTPs. **(Privileged & non-Privileged) ACME Portal Access:** ACME corp AppOps and Analysts roles have access to the ACME Portal Web Portal. All access to the ACME Portal requires UN/PW with Google Authenticator. **Customer Responsibility:** Customers do not have any privileged access to the components supporting the ACME Portal. Customer Administrators and Users are permitted access to the ACME Portal website. Customers may configure the portal to require MFA for all connections. MFA may be implemented in the following ways: • SAML integration with a customer IDP • Application UN/PW with Google Authenticator

2.3 Phase 3 - Assess

During this phase the SAP is prepared, an independent assessment is performed, Plans of Action and Milestones (POA&Ms) are developed, and a Security Assessment Report (SAR) is produced. Table 2-8 identifies the deliverables, activities, and responsibilities in this phase.

Table 2-8. Required 800-171 Deliverable Produced in this Phase

Deliverables	Activity	Responsibility
Security Assessment Plan (SAP)	The SAP is prepared, establishing the assessment expectations, the level of effort expected, and includes the: ● Current System Inventory Workbook ● GSA-CUI-Non-Federal-Test-Case-Workbook	Independent Assessor/Organization
Security Assessment Report (SAR)	The SAR is prepared based on the assessment. It must include: ● GSA-CUI-Non-Federal-Test-Case-Workbook and Supporting Artifacts ● Vulnerability Scanning Reports ● Configuration Scanning Reports ● Web Application Scanning Reports ● Penetration Test Report (as necessary)	Independent Assessor/Organization
Plan of Actions and Milestones (POA&M) CUI Nonfederal System Vulnerability Deviation Request Sheet (if needed)	The POA&M is prepared identifying planned actions to remediate any not fully implemented requirements and vulnerabilities identified in the SAR. A GSA Nonfederal System Vulnerability Deviation Request Sheet must be prepared for any Critical or High vulnerabilities or configuration deviations that the vendor cannot remediate.	Independent Assessor/Organization

2.3.1 Assessor Selection

The key to effective assessments is having assessors with the required skills, abilities, and technical knowledge to develop assessment plans, perform assessment testing, and prepare assessment reports. The assessment must be independent and completed by either a FedRAMP accredited 3PAO or by an assessment organization approved by the GSA OCISO prior to selection.

2.3.2 Security Assessment Plan

The assessors must develop and obtain approval of an SAP which will be leveraged to assess the security and privacy requirements. The purpose of the SAP approval is two-fold: (1) to establish the appropriate expectations for the security control assessment; and (2) to bound the level of effort for the security control assessment. The SAP will provide system background information, the objectives for the security assessment, the assessment approach, and use of the CUI Nonfederal System Test Case Workbook—an attachment to the SAP. The SAP must be approved by the Vendor System Owner, Vendor Security Officer, GSA ISSO, and GSA ISSM before assessment activities begin or the vendor is at risk of retesting.

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

The following security assessment requirements must be defined in the SAP and implemented for all information systems:

- **Security and Privacy Requirements Assessment.** The assessment of the NIST SP 800-171 and 800-172 requirements, and 800-53 controls (if PII is in scope) will be carried out using the GSA-CUI-Non-Federal-Test-Case-Workbook. Assessments will include examining relevant documentation, interviews, and technical/operational testing to verify requirements are in place and operating as intended.
- **Vulnerability Scanning - Operating System, Network Infrastructure, Container, and Database.** Vulnerability scanning can be performed either by the vendor's security team and/or independent security assessor. Vulnerability scanning shall be 1) authenticated and 2) encompass either the full system or a representative subset of the system, considering all device types. If the latter, scanned servers/applications must be clearly identified in relation to the full inventory and a rationale for the selection of this subset must be provided. This is completed for each scan type (OS/Network Infrastructure/Container/Database) and must be clearly defined in the SAP. Representative scans typically require 10% of devices and must cover all component types. Details pertaining to tooling, authentication, and in-scope populations will be required to be defined in the SAP. The scan configuration shall be provided along with the scan report and included in the assessors' evidentiary documents.
- **Configuration Scanning - Operating Systems, Network Infrastructure, Containers, Databases.** Configuration scanning can be performed either by the vendor's security team and/or independent security assessor. Configuration scanning shall be 1) authenticated and 2) encompass either the full system or a representative subset of the system, considering all device types. See Vulnerability Scanning above for details on acceptable representative subsets.

  Configuration/compliance scans shall be to NIST guidelines, CIS guidelines, or industry best practice guidelines, as deemed appropriate and mutually approved through the executed SAP. Where a CIS benchmark exists, configuration scanning must be to the benchmark. Any scanning tool configured to support the benchmarks or guidelines identified may be used.

  Clearly identify the compliance scans versus the vulnerability scans. Configuration scanning – must meet the minimum 85% compliance threshold (i.e., each component meets 85% of its configuration requirements). Configuration deviations from established benchmarks shall have defined exceptions with justification indicating why an exception

is needed to the setting. General justification statements will not be accepted (e.g., configuration setting not applicable).

- **Web Application Vulnerability Scanning.** Web application scanning can be performed either by the vendor's security team and/or independent security assessor. Web application scanning shall be authenticated and reflect all in-scope URLs. Testing is performed from external scanning systems against the information system using a variety of automated and manual scanning tools. The main purpose of the web application vulnerability scan is to discover and enumerate any deficiencies in the exposed web interface that could be leveraged by an attacker to gain unauthorized access to systems or data. Web application scanning focuses on the Open Web Application Security Project (OWASP) Top Ten Most Critical Web Applications Security Vulnerabilities, latest update. The vendor shall utilize industry standard tools (e.g., HP WebInspect, Netsparker, etc.) for web application scanning.
- **Penetration Testing (Recommended).** Penetration testing is recommended for Internet accessible information systems. Guidance on penetration testing is available in CIO-IT Security-11-51: Conducting Penetration Test Exercises.

Any Critical/High vulnerabilities identified during assessment activities must be remediated or mitigated. When Critical/High vulnerabilities are identified during the assessment activities, every effort shall be made to re-assess those vulnerabilities to verify that implemented strategies have adequately reduced the associated risks.

2.3.3 Assessment Requirements

Nonfederal information systems must have an independent assessment performed every three (3) years or whenever there is a significant change to the nonfederal system's security posture. Assessment activities begin after the SSPP has been mutually approved by the GSA security team and vendor and the SAP has been mutually approved by the GSA security team, vendor, and independent security assessor.

The assessment must be completed in a timely fashion. The expected timeline for the assessment could be delayed without a full commitment from all parties or prompt remediation of deficiencies identified during the assessment. The following sections describe key components of the independent security assessment and their related considerations.

2.3.4 Security Assessment Report

Assessors prepare a SAR documenting the issues, findings, and recommendations of the security control assessment (including, if applicable, a penetration test report as an attachment). The SAR documents the assessment findings with recommendation(s) and risk determinations based on NIST SP 800-30, Revision 1, "Guide for Conducting Risk Assessments." The SAR must individually identify and discuss findings as follows:

- Security and Privacy Requirements Assessment - All findings.
- Vulnerability Scanning - Critical, High, and Moderate findings.
- Configuration Scanning - Configuration scanning must be to approved baseline(s) and is expected to meet the minimum 85% compliance threshold. Configuration gaps can be detailed individually or grouped as a single finding with reference to the configuration scan file.
- Web Application Scanning - Critical, High, and Moderate findings.
- Penetration Testing (if performed) - All findings. Informational findings may be ignored.

The SAR will be included as part of the authorization package. The risk assessment should consist of the following steps:

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

Assessments must include vulnerability description, assessed risk, and recommendations for correcting the vulnerability. The SAR must be approved by the independent assessor.

2.3.5 Remediation Actions

The vendor will conduct initial remediation actions on security and privacy requirements based on the findings and recommendations of the SAR and reassess remediated requirement(s), as appropriate. Findings that are remediated should be appropriately marked in the SAR. In the SAR, include “Mitigated” or “Resolved” next to the heading for remediated requirements. Similarly, any findings proven to be a false positive should be identified as “False Positive” with a supporting justification statement. Additional instructions are provided in Appendix I and the SAR template.

2.3.6 Deviation Requests

Any Critical or High vulnerabilities or configuration deviations that the vendor cannot remediate must be captured in the Deviation Request Tracking Sheet.

1. Vulnerabilities that the vendor is unable to remediate.
2. Vulnerabilities that the vendor wishes to risk adjust.
3. Vulnerabilities identified as a false positive.
4. Deviations from the Secure baseline configuration identified by scanning.

All must be identified as such in the Findings Discussion of the SAR with supporting justification statements that are verified by the assessor. Deviations must be reviewed and accepted by the GSA, ISSO, ISSM, and CISO.

For all satisfied test cases, risk-based decisions (recommended by provider/accepted by GSA), and mitigated results, evidentiary artifacts must be supplied.

2.3.7 Plan of Actions and Milestones (POA&M)

The POA&M describes how the vendor intends to address identified vulnerabilities (i.e., mitigate, eliminate, or accept vulnerabilities). The assessor prepares the POA&M based on the findings and recommendations in the SAR excluding any remediation actions taken. The

POA&M must include all vulnerabilities except those identified as “Mitigated” or “Resolved” in the SAR. Use the GSA provided POA&M template (see Appendix B).

Update the SSPP to reflect the results of the security assessment and any modifications to the security and privacy requirements in the information system. The SSPP should reflect the actual state of the security and privacy requirements implemented in the system following completion of security assessment activities. This is necessary to account for any modifications made to address recommendations or corrective actions from the security assessor.

Note: For every Open or Outstanding finding in the SAR there must be a related planned action in the POA&M and in the SSPP for that NIST SP 800-171 security requirement or NIST SP 800-53 privacy control. Reference Table 2-7, Security and Privacy Requirements Discussion Statement (#2) for an example for properly capturing planned actions in the SSPP.

2.3.8 GSA Review

GSA IS and privacy staff will review the completed Security Assessment Report and supporting artifacts, the POA&M, and updated SSPP for completeness and accuracy. This review is intended to ensure:

- The security requirement and privacy control assessment was completed in accordance with the mutually agreed to Security Assessment Plan.
- The SAR and POA&M reflect all findings from the GSA CUI Nonfederal Test Case Workbook, vulnerability scanning, configuration scanning, web application scanning, and penetration testing (if applicable).
- Scans were authenticated, encompassing either the full system or the representative that was mutually agreed in the Security Assessment Plan, and include the scan configuration used along with the actual scan reports.
- Evidentiary Artifacts are captured that support the Assessment Result in the GSA CUI Nonfederal Test Case Workbook.

To increase the efficacy of the review, SAR findings, POA&Ms, and evidentiary artifacts should be itemized with a unique identifier that binds the necessary relationships together. For instance, a satisfactory assessment coupled with an evidentiary artifact should use the same unique identifier to bind the relationship. GSA recommends creating a reference matrix that depicts these relationships.

Any concerns will be identified by the GSA security team and raised to the Vendor and Assessor for remediation.

2.4 Phase 4 - Authorize

The process described in this phase is used by GSA to ensure CUI processed, transmitted, or stored on nonfederal systems is appropriately protected. The purpose of the review is to ensure the approval package clearly and accurately reflects the security posture of the vendor's information system in order for the GSA to make an informed risk-based approval decision.

During this phase, the vendor assembles the Nonfederal System Security Approval Package listed in Appendix B and submits it to the GSA ISSO, ISSM, and COR for review and approval consideration. The GSA security team then conducts a quality and risk review of the vendor's Nonfederal System Security Approval Package. The outcome of the review may result in a

detailed set of comments to address inconsistencies in the approval package. If such is the case, the vendor and/or the 3PAO/independent security assessor may be required to address documentation gaps or inconsistencies identified by the agency review team. Examples include:

- Inconsistencies across SSPP control narratives.
- Inconsistencies between the boundary diagram, data flow diagrams, and SSPP narrative.
- Inconsistencies between control narratives and what is validated by the 3PAO/independent security assessor and described in the GSA Nonfederal CUI Test Case Workbook.
- Inconsistencies between the SAR and POA&M.

In addition, the vendor may be asked to remediate or mitigate open risks in order to achieve an acceptable level of risk for the GSA. In some cases, the 3PAO/independent security assessor may be required to perform delta testing to validate risk remediations or perform additional testing if the agency review team identifies gaps in the initial assessment scope. For example, if the 3PAO/independent security assessor failed to validate the encryption status of federal data/metadata at rest and in transit, or failed to test a component essential to the operation of the vendor's information system.

Upon remediation of GSA identified comments and vendor delivery of the updated Nonfederal System Security Approval Package, the GSA security team finalizes its review of the approval package and transmits the approval package including the required deliverables in Appendix B to the GSA CISO (and CPO if PII is in scope) for approval consideration.

This phase does not result in a traditional Authority to Operate (ATO) as described in the RMF Authorize step in NIST SP 800-37. GSA will prepare a Memorandum for Record (MFR) concerning the use of the vendor system. The memorandum is based on the evidence provided in the Nonfederal System Security Approval Package and is the result of the following steps.

1. The GSA ISSO assembles the Nonfederal System's Security Approval Package and submits it to the GSA ISSM certifying the vendor system has met the process requirements described in this guide and the residual risk is acceptable.
2. The GSA ISSM will review the package to validate the GSA ISSOs certification and residual risk determination. Incomplete packages or packages inconsistent with the requirements in the guide will be returned to the ISSO to be corrected. Complete packages consistent with the requirements in this guide with acceptable levels of residual risk will be forwarded to the GSA CISO (and CPO if PII is in scope) along with the MFR for review and approval consideration.
3. The GSA CISO (after coordination with CPO if PII is in scope) will inform the GSA ISSM and ISSO:
    a. To update the package if it needs additional work; or,
    b. Will execute the MFR for the system's use if the package provides sufficient evidence CUI is appropriately protected by the Nonfederal System.

Table 2-9 identifies the deliverables, activities, and responsibilities in this phase.

Table 2-9. Required 800-171 Deliverable Produced in Phase 4

Deliverable	Activity	Responsibility
Final CUI Nonfederal System Security Approval Package See Appendix B	The complete approval package is assembled, reviewed, and approved.	Vendor assembles, GSA assists

2.5 Phase 5 Monitor

Once a vendor achieves approval of its GSA Nonfederal System's Security Approval Package, the vendor must continuously monitor the security posture of its information system offering; and provide GSA with information needed to make risk-based decisions about its ongoing approval.

The monitor phase is the key factor in tracking the security of CUI in nonfederal systems over time. The vendor shall create, maintain, and update the security documents identified in the following sections, at the frequencies described, and provide them to the Government.

This phase consists of using continuous monitoring of the system and its security and privacy requirements to ensure they continue to satisfy security and privacy requirements. Continuous monitoring activities and deliverables assist in determining if the security and privacy requirements in the information system continue to be effective over time considering changes that occur in the system and environment. Through continuous monitoring, evidence of meeting security and privacy requirements, including supporting deliverables, are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information system(s). They allow GSA to make credible risk-based decisions regarding the nonfederal system and initiate appropriate responses as needed when changes occur.

2.5.1 Quarterly Deliverables

The following deliverables are to be provided to the GSA ISSO, ISSM, and/or Contracting Officer (COR) on a quarterly basis:

1. **Vulnerability Scanning Reports** - reference NIST SP 800-171, security requirement 3.11.2 "Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified." Provide the most recent web application and operating system vulnerability scan reports.
2. **POA&M Update** - reference NIST SP 800-171, security requirement 3.12.2 "Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems." Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)."
3. **Shared Drive Access Review** - The Vendor and GSA ISSO shall review the membership and access to the shared collaboration drive.

Quarterly Deliverables are due one month prior to the completion of each quarter in the government fiscal year, ending on September 30. Due dates are the last workday of the months listed:

- **Quarter 1 – November**
- **Quarter 2 – February**
- **Quarter 3 – May**
- **Quarter 4 – August**

2.5.2 Annual Deliverables

The following deliverables are to be provided to the GSA ISSO, ISSM, and/or COR on an annual basis (or when there is a major change to the system):

1. **Updated SSPP** - reference NIST SP 800-171, security requirement 3.12.4 "Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security and privacy requirements are implemented, and the relationships with or connections to other systems." The SSPP must be in accordance with NIST SP 800-171, using the SSPP template provided by the GSA.
2. **Updated PTA/PIA** - the privacy posture of the nonfederal system and its environment of operation will be validated via annual reviews (including the SAR listed above), and updates as necessary, to the PTA/PIA.

3. **Penetration Test –** Penetration testing is **recommended** for Internet accessible information systems. Guidance on penetration testing is available in the CIO-IT Security-11-51: Conducting Penetration Test Exercises.

Annual deliverables are due two months prior to completion of the government fiscal year, ending on September 30. The due date is the last workday of July.

2.5.3 Deliverable Provided Every Three Years

The following deliverable is to be provided to the GSA ISSO, ISSM, and/or COR every three years (or when there is a major change):

- **SAR,** reference NIST SP 800-171, security requirement 3.12.1, Security Assessment. Deliver the results of the security assessment conducted by a 3PAO/independent security assessor using the assessment procedures in NIST SP 800-171Ar3, "Assessing Security Requirements for Controlled Unclassified Information", to be completed using the SAR template provided by the GSA. The SAR is completed in accordance with a security assessment plan that is mutually agreed upon by the GSA, the vendor, and the 3PAO/independent security assessor following the process requirements in this guide.

The SAR deliverable is due two months prior to completion of the government fiscal year, ending on September 30. The due date is the last workday of July.

2.5.4 Major Changes requiring pre-notification:

The following types of Major Changes require pre-notification and acknowledgement by the GSA ISSO, ISSM and CO/COR prior to their implementation. These changes may require re-assessment:

- Changes to the CUI data types and retention by the system.
- Changes to the encryption used to protect GSA CUI data at rest or in transit.
- Re-hosting or re-platforming the system including migrations to different data centers, to the cloud, or between cloud providers.
- Addition of any External Service that may store, process or transmit CUI.
- Removal of security components used to protect and monitor the information system.
- Removal of MFA requirements for administrative access to the system or GSA CUI data.

2.5.5 All Other Changes

The following changes will require documentation updates and should be clearly outlined and in the quarterly Continuous Monitoring deliverables and discussed with the GSA ISSO and ISSM. These changes MAY require re-assessment:

- New features/capabilities provided to GSA.
- Replacement of security components used to protect and monitor the information. system, including scanning tools, antivirus software, firewalls, VPN solutions, etc.
- New authentication mechanisms or changes to existing mechanisms.
- New system monitoring capabilities or replacement of system monitoring capabilities.

3 Incident Response

Vendors are required to comply the CIO-IT Security-01-02: Incident Response for reporting any incident (suspected or confirmed) that results in the actual or potential loss of confidentiality, integrity, or availability of the vendors information system offering or the data/metadata that it stores, processes, or transmits. Reporting real and suspected incidents allows GSA and other affected customers to take steps to protect important data, to maintain a normal level of efficiency, and to ensure a full resolution is achieved in a timely manner.

Incidents or suspected incidents do not result in punitive actions against a vendor. However, failure to report incidents will result in escalation.

3.1 Incident Reporting

Vendors must report all incidents, which include suspected or confirmed events that result in the potential or confirmed loss of confidentiality, integrity, or availability to assets or services provided by the in the system boundary. Incidents must be reported to the GSA ISSO, ISSM, COR, and GSA Incident Response Team at GSA-IR@gsa.gov **within one hour** of being identified by the vendors top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or information technology department. Do not delay reporting in order to collect additional details. The following information must be captured in the incident report:

1. Identify the current level of impact on agency functions or services (Functional Impact).
2. Identify the type of information lost, compromised, or corrupted (Information Impact).

3. Estimate the scope of time and resources needed to recover from the incident (Recoverability).
4. Identify when the activity was first detected.
5. Identify the number of systems, records, and users impacted.
6. Identify the network location of the observed activity.
7. Identify point of contact information for additional follow-up.

The following additional information should also be included if known at the time of incident reporting:

8. Identify the attack vector(s) that led to the incident.
9. Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident.
10. Provide any mitigation activities undertaken in response to the incident.

Vendors must maintain current and accurate contact information on file for their GSA ISSO, GSA ISSM, GSA COR, and GSA Incident Response Team at GSA-IR@gsa.gov. Upon incident reporting to the GSA, the GSA Incident Response Team will initiate an incident and perform follow-on reporting to US-CERT and the GSA Office of the Inspector General. If necessary, GSA will work with the vendor to notify agency customers. Additional direction will be provided by the GSA Incident Response Team and/or the GSA ISSO/ISSM.

Appendix A: References

Federal Laws, Standards, Regulations, and Publications:

The contractor shall comply with the following:

- CUI Regulation 32 CFR Part 2002, Controlled Unclassified Information (CUI)
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS PUB 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 800-53A, Revision 5, Assessing Security and Privacy Controls in Information Systems and Organizations
- NIST SP 800-60, Volume I, Revision 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-60, Volume II, Revision 1, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST 800-63B-4, Digital Identity Guidelines, Authentication and Lifecycle Management
- NIST SP 800-161, Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- NIST SP 800-171r3, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- NIST SP 800-171Ar3, Assessing Security Requirements for Controlled Unclassified Information
- NIST SP 800-172r3 (Draft), Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171
- NIST SP 800 172Ar3 (Draft), Assessing Enhanced Security Requirements for Controlled Unclassified Information
- Title 44 U.S. Code, Sec. 3554, Federal agency responsibilities

GSA Policies, Procedures, and Guidance:

The contractor shall comply with the following:

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

- GSA Order CIO 1878.3, Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices
- GSA Order CIO 2100.1, GSA Information Technology (IT) Security Policy
- GSA Order CIO 2103.1, Controlled Unclassified Information (CUI) Policy
- GSA Order CIO 2200.1, GSA Privacy Act Program
- GSA Order CIO 9297.2, GSA Information Breach Notification Policy

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

- GSA CIO-IT Security-11-51: Conducting Penetration Test Exercises (Recommended)

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

- GSA CIO-IT Security-01-02: Incident Response
- GSA CIO-IT Security-09-44: Plan of Action and Milestones (POA&M)

Appendix B: Nonfederal System Security Process Documents

Table B-1 contains a listing of the security approval package documentation required for protecting CUI in nonfederal systems and organizations. Table B-2 contains a listing of deliverables and job aids used throughout the 800-171 process that are not part of the security approval package. Templates for all items listed in both tables are accessible to personnel with GSA accounts and GSA Affiliated Customer Accounts (GACAs). The GSA ISSM/ISSO can provide the documents and job aids, if necessary.

Table B-1. Protecting CUI in Nonfederal Systems Security Package

Document Name and Link	RMF Phase
CUI Nonfederal System SSPP Template Attachment 1 - FIPS 199 Security Categorization Template Attachment 2 – CUI Nonfederal FedRAMP vs 800-171 Qualifying Template (Optional) Attachment 3 – CUI Nonfederal System Integrated Inventory, Leveraged and External Services Workbook Template Attachment 4 - CUI Nonfederal System PTA Template Attachment 5 - CUI Nonfederal System PIA Template - if required per the PTA Attachment 6 - CUI Nonfederal System Security Architecture Review Checklist Attachment 7 - CUI Nonfederal Systems SCRM Plan	 Prepare (Qualify) Prepare (Qualify) Document Document Document Document Document
CUI Nonfederal Systems SAR Template Attachment 1 – CUI Nonfederal System SAP Template Attachment 2 – GSA CUI Nonfederal Test Case Workbook Attachment 3 - OS/Container/Database scan data (as appropriate) Attachment 4 - OS configuration settings verification data Attachment 5 - Webapp scan data (as appropriate) Attachment 6 - CUI Nonfederal System Vulnerability Deviation Request Sheet (if necessary) Attachment 7 - Penetration Test Report (as necessary)	 Assess Assess
CUI Nonfederal Systems POA&M Template	Assess
CUI Nonfederal Memorandum for Record Template	Authorize

Table B-2. Additional Templates/Job Aids

Document Name and Link	RMF Phase
Job Aid – CUI Nonfederal Vendor Kickoff Overview Slides	Prepare
Job Aid – CUI Nonfederal System WBS (Optional)	Prepare
Job Aid - Example Control Statements (Available upon request)	Document

Appendix C: Showstopper Security and Privacy Requirements for the Nonfederal Security Approval Process

An assessment must be completed for the CUI requirements in the CUI Nonfederal Systems Requirement Tailoring Workbook based on applicability. Use the GSA CUI Nonfederal Test Case Workbook to record assessment results. The GSA security team is responsible for ensuring all the security requirements and privacy controls are assessed. Table C-1 below highlights security requirements that are showstoppers (i.e., will preclude approval if the requirement is not fully implemented).

Note: A number of the security requirements have organization-defined parameters. Below is an example of a control statement with no assigned parameter and the control statement after the parameter has been assigned. Each control with a parameter requiring an assignment **must have an assignment in the SSPP by the organization** (i.e., not assigned by GSA).

EXAMPLE:

g. Notify account managers and designated personnel or roles within:
1. [Assignment: organization-defined time period] when accounts are no longer required.

g. Notify account managers and designated personnel or roles within:
1. [14 days] when accounts are no longer required.

Table C-1. Protecting CUI in Nonfederal Systems Showstopper Security Requirements

Requirement Number	NIST Requirement Source	Requirement Title/ Description	Guidance (if applicable)
		Access Control	
03.01.02	800-171	**Access Enforcement** Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.	
03.01.12	800-171	**Remote Access** a. Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access. b. Authorize each type of remote system access prior to establishing such connections. c. Route remote access to the system through authorized and managed access control points. d. Authorize the remote execution of privileged commands and remote access to security-relevant information.	

Requirement Number	NIST Requirement Source	Requirement Title/ Description	Guidance (if applicable)
		Identification and Authentication	
03.05.03	800-171	**Multi-Factor Authentication** Implement multi-factor authentication for access to privileged and non-privileged accounts.	
		Risk Assessment	
03.11.02	800-171	**Vulnerability Monitoring and Scanning** a. Monitor and scan the system for vulnerabilities [Assignment: organization-defined frequency] and when new vulnerabilities affecting the system are identified. b. Remediate system vulnerabilities within [Assignment: organization-defined response times]. c. Update system vulnerabilities to be scanned [Assignment: organization-defined frequency] and when new vulnerabilities are identified and reported.	
		System and Communications Protection	
03.13.01	800-171	**Boundary Protection** a. Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system. b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. c. Connect to external systems only through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.	
03.13.08	800-171	**Transmission and Storage Confidentiality** Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.	Encryption of sensitive data (e.g., PII, PCI, Authenticators, other business sensitive data) at rest and in transit shall be with FIPS validated encryption modules wherever possible.

Requirement Number	NIST Requirement Source	Requirement Title/ Description	Guidance (if applicable)
03.13.11	800-171	**Cryptographic Protection** Implement the following types of cryptography to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography].	Encryption of sensitive data (e.g., PII, PCI, Authenticators, other business sensitive data) at rest and in transit shall be with FIPS validated encryption modules wherever possible.
		System and Information Integrity	
03.14.01	800-171	**Flaw Remediation** a. Identify, report, and correct system flaws. b. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates.	
		System and Services Acquisition	
03.16.02	800-171	**Unsupported System Components** a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer. b. Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.	

Appendix D: Boundary Diagram Guidance

An authorization boundary provides a diagrammatic illustration of the nonfederal systems' internal services, components, and other devices, along with connections to external services and systems. Please note that external services include external cloud services that are not FedRAMP-approved, Corporate Shared Services, and the external entities to which the system must connect to receive updates for products installed within the system boundary.

An authorization boundary accounts for all CUI information, data, and metadata that flow through the nonfederal system.

Common Mistakes:

- Failure to outline components with sufficient detail (See the guidance section below for more information)
- Failure to clearly identify CUI data flows
- "Black Box" services
- Failure to illustrate Admin Access interfaces, Jump Boxes, AWS consoles.
- Failure to illustrate other external services required by the system
- Failure to clearly identify CUI flows
- Failure to identify privileged user interactions
- Failure to identify authentication methods.

This example system diagram in Figure C-1 is provided to illustrate key concepts, it is not a complete diagram, nor does it capture all services that would be required by a system, i.e., Identity and Authentication and Security/Audit logging.

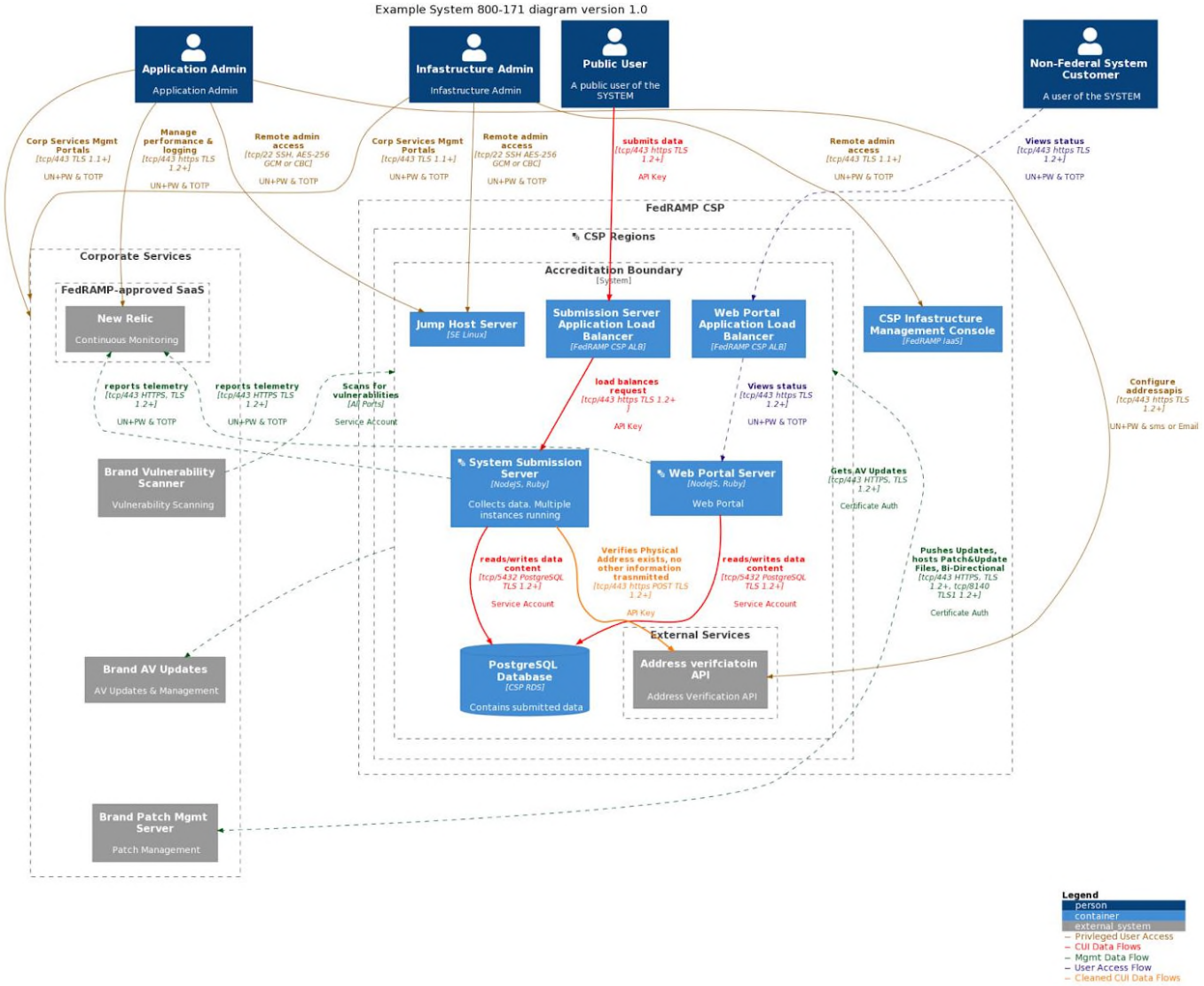

Figure D-1. Example System Diagram

Guidance:

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

- Provides an easy-to-read diagram that includes a legend. The Authorization Boundary Diagram (ABD) should be readable without having to enlarge it.
    - It is acceptable to provide the ABD as a separate attachment
    - It is acceptable to provide data flow diagrams that support or further illustrate the Boundary Diagram
- Includes a prominent border drawn around all components in the nonfederal system
    - This should include all components that handle process or store CUI data or metadata.
- 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. Inventory and Tables should easily be tracked to the architecture diagram.
    - This includes services used to manage and operate the system (e.g., SIEM, Vulnerability Scanning, System Monitoring, Ticketing)
    - Identify all depicted tools, services, or components as either external or internal to the boundary
    - If there are multiple instances of a given component performing the same function, i.e., 3 web application servers serving ExampleApp behind a load balancer, it is okay to identify the 3 ExampleApp servers in a single box.
- Depicts all ingress/egress points
- Depicts services leveraged from the underlying IaaS/PaaS and identify any services that are not FedRAMP authorized
    - Depending on the nature and type of integration and sensitivity of the data, these dependent systems may also need to be
- Depicts all interconnected systems and external services, including corporate shared services, and identifies any systems/services that are not FedRAMP authorized. Again, how you do this is up to you.
- Depicts how system admins and Agency customers access the vendor service (i.e., authentication used to access service).
    - If applicable, depicts components provided by the vendor, and installed on customer devices, as inside the authorization boundary.
    - These components are required to be in the boundary if they materially affect the Confidentiality of the CUI data (e.g., data collectors in customer data centers and mobile applications
- Ensure all authentication points (this includes but is not limited to AWS console, jump, machine resources, network devices, application, API, enablers, etc. (as applicable)), are defined. MFA 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 authentication shall be MFA; privileged authentication is required to be MFA for all FIPS impact levels.
- Shows connections between components within the boundary and to/from external services
    - For example, include connections from load balancers to the servers they support. Similar flows can be combined or noted (e.g., bastion server access to all hosts, all devices forward logs to log server, etc.)

  - Depicts dev/test environment, alternate processing site, and location of backups
  - The dev/test environment must be included within the boundary if federal CUI data and/or if federal government personnel have access to the environment for any reason, including training and user acceptance testing
- Shows update services (e.g., malware signatures and OS updates) outside the boundary.

Appendix E: Writing Security and Privacy Requirements Guidance

Writing should be clear and fully answer the Security Requirement

- This will speed up the review process by avoiding requests for clarification and re-writes
- Take the guesswork and assumption out of the writing. Write to it as the audience has no history, context, or experience with your system.
- Ensure the security requirement response covers all applicable components captured in the inventory and boundary diagram.
- Every statement should include “Who,” “What” Where,” “When,” “Why,” and “How.”
- Explain who is responsible for implementing the solution, roles should be consistent though the document
- Explain what the system does to implement the security requirement
- Explain where the implementation happens (e.g., location, alternate locations)
- Explain when the solution is appropriate. (e.g., when an employee leaves, on a monthly basis”
- Explain why a certain action is taken (e.g., this action addresses this part of the security requirement)
- Explain how the system uses certain tools or capabilities
    - If the security requirement says, “test x,” You can’t just say “Yes, we test x.” You must say <role name> test X <frequency> using <tool name>”

Clear

- Content is unambiguous and simply stated
- Written in correct and consistent format
- Logical presentation

Concise

- All content is relevant to the subject
- Complexity level is suited to the audience
- No use of superfluous words or phrases

Consistent

- Terms have the same meaning throughout the document
- The level of detail and presentation style is the same throughout the document

Complete

- Responsive to all applicable requirements
- Security Package includes all appropriate sections of the Template
- Security Package includes all attachments and appendices
- Covers all components in the diagram and inventory
- Includes all roles and groups
- Consistent language and completeness when referring to components (tied to diagram and inventory)
    - If describing the patching process, it should cover all components, not just the app or

- Consistent language and completeness when referring to roles or groups.

Please Don't Do This:

- Don't repeat or rephrase the security requirement instead of answering how it is implemented.
- Don't use boilerplate text, copied and pasted over and over again.
- Don't include text not directly relevant to describing how the security requirement is implemented.
- Don't leave blank areas. For example, no security requirement implementation description has been written.
- Don't mark an item N/A when that is not the case, or mark it N/A without a detailed explanation of why it is considered N/A.
- Don't use empty words like "world-class," "user-friendly," or "-related."
- Don't use the phrase "such as," security requirement statements need to be explicit.
- Don't inappropriately cite a document (the "it's in there somewhere" technique) instead of describing specifically how the security requirement is implemented.
- Where a document citation is appropriate to indicate some part of an implementation, provide the title, version, and date (and section or page of the document containing the specifics).

Avoid the Passive Voice:

- Passive voice: "The Report is sent to the customer."
- Active voice: "The Project Manager sends an e-mail with the Weekly Status Report to the Program Director on the first business day of every week by 3:00PM."
- The active voice tells who is taking the action.
- In addition, you must tell the entire story: what is sent, when it is sent, how it is sent, and any other information needed to tell the entire story.
- If your sentence makes grammatical sense when you add the words "by zombies" after the verb, then you are writing in passive voice, and must switch to active voice.

Please Do This:

- Do write complete sentences, with subject, verb, and direct object.
- Do break up long sentences into several shorter ones.
- Do prefer simpler words to longer words, as long as no meaning is lost.
- Do stick to one verb tense. Prefer the simple present tense unless you truly are referring to the past or future.
- Do write in the active voice and use action verbs.
- Do make generous use of vertical white space for bulleted and numbered lists. Use a list for four or more items. Consider it for three.
- Do be sure you understand every word, abbreviation, or acronym you write.

Appendix F: Remote Access Guidance

One of the most critical components of a secure architecture is privileged remote access and systems administration. Remote access and administration safeguards are critical because a compromise of a weak front end or poor integration with a corporate active directory could result in lateral movement into the authorization boundary. Integration of information systems with services such as corporate Active Directory is generally discouraged unless proper safeguards can be implemented. Below are several safeguards and best practices that should be adhered to in designing a secure remote administration capability.

GSA will review privileged remote access as part of the Architecture Approval process. If vendors have questions regarding their proposed solution, it is advised to discuss and obtain approval during the initial engagement to avoid any re-engineering.

1. The authorization boundary should be logically and physically isolated from corporate networks and other information systems by utilizing firewall technology; VLANs may be acceptable but are prone to more risk.
2. If implementing Directory Services (DS), the assets/devices in scope of the System boundary should be tied to DS that is separate from that used in the corporate network. This is the most secure setup and limits lateral risk.
3. If utilizing a Federated account to access assets/devices in scope of the authorization boundary, the initial connection through VPN or Jump server should present a new MFA challenge and not directly log in. Also, please document the token expiration time frame of any Federated access.
4. Use a Jump server (or like solutions (to be approved on a case-by-case basis)) to authenticate into the system boundary. If using DS; the Jump server should be tied to the DS in the system boundary; not the corporate network. This is the most secure setup.
5. The jump box should not utilize a persistent connection. A non-persistent and unique session should be invoked at logon. The goal is to take the connecting laptop out of the risk equation.
6. Access to the jump box should be restricted via access control lists or policies; ideally limited to defined IP addresses/subnets/VLANs via IP Filtering (not the entire network and never from the Internet) and/or device certificate authentication.
7. The Jump Server should not be publicly accessible, only available from corporate networks via ACL or certificate, or from a VPN connection.
8. If connecting from a VPN, the VPN client shall implement MFA technology that is phishing resistant (OTP pin sending via email is prohibited and SMS is restricted as they are prone to intercept risk) and utilize credentials other than those used to access the Jump server.
9. IF VPN is used, ensure the VPN does not allow split tunneling of VPN traffic.
10. Authentication to the jump box should utilize dedicated accounts, either tied to a corporate active directory or active directory within the authorization boundary; the latter is more secure.
11. Authentication to the jump box must prompt for logon and not pass-through credentials as single sign on from a corporate active directory.
12. MFA should be configured and enforced at the user object; not at the device-level.
13. Connection to the jump box and subsequent connections to managed assets and all authentication points must use encrypted communication.
14. The jump box should be configured to launch a new connection to managed assets from the jump box itself and not the administrator's workstation.

Appendix G: Scanning Guidance

Table G-1. Scanning Guidance

Component Type	Recommended Minimum Scanning Frequency	Required Reporting Timeline
Operating System (OS) Vulnerability Scan	Weekly authenticated scans for servers and appliances where major OS is used (Unix, Windows, or major Linux distribution), unauthenticated scans for hardened appliances and other devices.	Quarterly Scanning Deliverables (reflecting the latest scan) are due one month prior to the completion of each quarter in the government fiscal year, ending on September 30. Due dates are the last workday of the months listed: ● Quarter 1 – November ● Quarter 2 – February ● Quarter 3 – May ● Quarter 4 – August **Note** Recommended minimum security frequencies are just that; they can be more frequent. See Section 2.5 Phase 5 Monitor for detailed Continuous Monitoring Requirements to the GSA.
Container Image Scanning	Vulnerability and Compliance Scanning and periodic re-scans on a monthly basis.	
Container Configuration Guidance	Biweekly Authenticated scan for Containers and Container Platforms.	
OS Config Scan	Biweekly Authenticated for Servers N/A for appliances and proprietary devices where hardening guides do not exist or apply.	
Database Config Scan	Biweekly Authenticated for Servers N/A for appliances and proprietary devices where hardening guides do not exist or apply.	
Web Application Scan	Monthly Authenticated for URLs where public facing login exists Monthly unauthenticated otherwise.	
Database (DB) Vulnerability checks are normally part of OS scans. If they are not, use the following frequency	Weekly Authenticated unless flat file or proprietary database.	
Penetration Test	Recommended	If completed, submit annually two months prior to completion of the government fiscal year, ending on September 30. The due date is the last workday of July.

Appendix H: Container Guidance

This appendix provides additional guidance to the processes, architecture, and security considerations specific to cloud systems using container technology. Any requirement a vendor is unable or unwilling to meet must be submitted to GSA for risk acceptance consideration.

- Hardened images must be used. They must:
  - Contain the minimum software needed to perform their function.
  - Hardened to appropriate CIS Level 1 benchmarks where available.
  - Have SSH disabled.
  - A 3PAO must validate that the hardened image meets applicable CUI Nonfederal system requirements.
  - A 3PAO must validate the vendor's process of hardening images intended for deployment.
  - Include a unique asset identifier which corresponds to one or more production-deployed containers. These image-based asset identifiers must be documented in the CUI Nonfederal System Integrated Inventory, Leveraged and External Services Workbook Template.
- Automated container orchestration tools must be used to build, test, and deploy containers to production. They must include:
  - Role Based access control with MFA.
  - Registry monitoring and image verification.
  - Implement Policy-based micro segmentation to include the ability to segment traffic between Containers, Pods, and Namespaces.
  - Changes to orchestration (Kubernetes, etc.) or individual containers must be followed by a peer review process and continuously monitored.
  - Vulnerability scanning prior to being placed in production, when possible.
  - A 3PAO must validate the automated tools meet applicable CUI Nonfederal system requirements.
- Containers must be scanned for vulnerabilities.
  - See Appendix G.
- Runtime and Monitoring of containers must include:
  - Security Sensors that provide visibility into running containers and platforms. Containers, Orchestration Software, and Orchestration Network must be monitored for anomalous behavior.
  - Logging from container, nodes, and orchestration environments to a central SIEM.
  - A documented process for auditing and reviewing logs and events from the orchestration environment.
- Vulnerability Management
  - Both nodes and containers should be patched to remediate vulnerabilities.

Appendix I: False Positive Reporting Guidance

Below is some guidance on False Positive Reporting:

- Sufficient, supporting documentation should be provided with the false positive request.
- When requesting that a vulnerability be considered a false positive, the detailed documentation shows the steps that were followed and the tests that were used (including input/outputs and screenshots) to validate that a vulnerability is a false positive.
- The documentation should allow an independent validation that the vulnerability does not in fact apply to the specific host.
- A ticket should be opened with the scan tool vendor to determine why it is flagging a host as vulnerable. The vendor response should be captured as an artifact.
- If a vulnerability is considered to be a false positive, there should be some communication with the scan tool vendor (e.g., Tenable) to perform troubleshooting and determine why the vulnerability is being flagged. This can help resolve the false positives by improving the tool's vulnerability detection, identify changes to the scanning methodology, or identify configuration changes on the hosts to avoid the false positives. The false positive request should include the ticket number that has been opened with the scan tool vendor.
- All aspects of the vulnerability being considered should be reviewed prior to submitting for consideration as a false positive.
- The "Plugin Output," "Description," and "Synopsis" fields often include important information for determining the reason that a vulnerability has been flagged or the steps that need to be taken to resolve the vulnerability. For instance, some Windows patches introduce a new security feature, but a registry setting needs to be set in order to enable that feature. In this case, the plugin output would indicate that the patch has been applied but the registry entry still needs to be set.