



GSA CUI Phase 2 Documentation Checklist

Get Your First Submission Right

The Reality: Most federal contractors submit Phase 2 documentation once, get feedback that it doesn't meet GSA standards, and have to resubmit—adding 8-12 weeks to their authorization timeline[1].

The Opportunity: Contractors who understand exactly what GSA reviewers expect save weeks of rework and accelerate their path to assessment.

This checklist extracts what "good documentation" actually looks like according to CIO-IT Security-21-112, Revision 1[1]. Use it to audit your Phase 2 package before submission.

Phase 2 Overview: Two Critical Submission Windows

GSA divides Phase 2 into two distinct reviews[1]:

Phase 2a: Initial SSPP Submission (Sections 1-2 + Showstoppers)

- **Focus:** System boundary, architecture, and Showstopper requirements
- **Timeline:** 4-6 weeks to prepare; 2-4 weeks GSA review
- **Deliverables:** Limited, architecture-focused
- **Gate:** Must be approved before Phase 2b can begin

Phase 2b: Complete SSPP Submission (All Requirements)

- **Focus:** Full security and privacy requirements documentation
- **Timeline:** 4-8 weeks to prepare; 4-6 weeks GSA review
- **Deliverables:** Complete SSPP, all attachments
- **Gate:** Must be approved before Phase 3 (Assessment) can begin

Critical Point: Getting Phase 2a approved on first submission can save 4-8 weeks[1].

Deliverables Checklist: What Must Be Submitted

Phase 2a: Initial Submission Deliverables

- SSPP Sections 1 & 2** - System information and system environment
 - Architecture Diagram and Boundary Definition** - Comprehensive system boundary visualization
 - Showstopper Requirements (Appendix C)** - Only the 7 critical requirements in Section 3
-



GSA CUI Phase 2 Documentation Checklist

- Integrated Inventory, Leveraged and External Services Workbook** - Complete asset and service inventory
- System Security Architecture Review Checklist** - Verification of architectural elements
- Privacy Threshold Assessment (PTA)** - Required for all systems
- Privacy Impact Assessment (PIA)** - Conditional, only if PTA indicates PII processing

Phase 2b: Complete Submission Deliverables

- Updated SSPP Section 3** - All security and privacy requirements (not just Showstoppers)
- Supply Chain Risk Management Plan** - Vendor assessment and third-party risk documentation
- Updated Architecture and Inventory** - Any changes since Phase 2a approval
- All Supporting Evidence** - Documents referenced in requirement narratives

System Boundary Definition: The Foundation

Your authorization boundary diagram is everything. It determines what gets assessed and how[1]. GSA reviewers will scrutinize this against your SSPP and inventory.

Boundary Diagram Essentials Checklist

- Prominent border** - Clear, visible border around ALL components in scope
- System components detailed** - Every asset, device, service (physical and virtual)
- Protected enclaves separated** - Distinct borders for protected enclaves, subnets, DMZs
- External connections shown** - All integrations with SaaS, APIs, corporate network, external systems
- Data flows identified** - CUI data flows clearly marked and distinguished from other traffic
- Source/destination labeled** - All flows labeled with source, destination, ports, protocols
- Encryption status indicated** - Each data flow marked as encrypted or unencrypted
- Access controls depicted** - All firewalls, ACLs, proxies, network controls shown
- Authentication points marked** - Every login point identified (cloud console, jump host, app, API)
- MFA indicators present** - MFA requirements visible at each authentication point



GSA CUI Phase 2 Documentation Checklist

- Leveraged services differentiated** - FedRAMP vs. non-FedRAMP services clearly identified
- COOP/DR integrated** - Disaster recovery and continuity sites in scope if applicable
- Test/dev environments included** - Testing and development systems shown if in boundary
- Monitoring tools depicted** - SIEM, vulnerability scanners, antivirus, IDS/IPS included
- Admin access shown** - How administrators access the system from outside boundary
- Legend provided** - Clear legend explaining symbols and components
- Readable at normal size** - Diagram legible without enlargement (acceptable to provide as separate attachment)

What GSA Reviewers Look For in Boundary Diagrams

Sufficient Detail:

- Components are not "black boxes"
- Internal flows within components are visible
- All authentication points are explicit
- Every data flow has source, destination, port, protocol identified

CUI Data Flows:

- CUI flows are explicitly marked and distinguished from other traffic
- Unencrypted flows have explicit justification
- Data sensitivity is clear for each flow
- Government vs. non-government data is differentiated

Completeness:

- Every system component from the inventory appears in the diagram
- Every external service integration is depicted
- Every access method (privileged and non-privileged) is shown
- Every security tool (SIEM, scanner, antivirus, firewall) is included

Common Rejection Reasons:

- Components shown as simple boxes without internal detail or flows
- Missing authentication point identification
- Failure to distinguish CUI flows from other network traffic



GSA CUI Phase 2 Documentation Checklist

- Jump hosts/bastion servers not depicted
- Admin access interfaces not documented
- FedRAMP vs. non-FedRAMP services not differentiated
- Encryption status not indicated on data flows
- Prohibited vendor technology depicted in diagram

System Inventory Requirements

Your system inventory must align perfectly with your architecture diagram[1].

Integrated Inventory Checklist

- Hardware inventory complete** - All servers, appliances, network devices, workstations
- Software inventory complete** - All operating systems, applications, libraries, services
- Virtual components listed** - All VMs, containers, cloud instances, orchestration platforms
- Vendor information** - Vendor name and contact for each component
- Support status verified** - End-of-Life (EOL) status confirmed for each component
- Version numbers documented** - Current version for all software and services
- URLs documented** - For all web services and external integrations
- Data types identified** - What data each component stores, processes, or transmits
- CUI sensitivity marked** - Components that touch CUI clearly marked
- External services tab complete** - All SaaS, IaaS, PaaS integrations documented
- FedRAMP status indicated** - Each external service marked as FedRAMP authorized or not
- Leveraged services justified** - Non-FedRAMP services have GSA risk-basis approval documented
- Prohibited vendors checked** - Verification that Kaspersky, Huawei, ZTE, Hikvision, Hytera, Dahua not present
- Consistency verified** - Inventory items match architecture diagram components

External Services Tab Specifics

For each external service (SaaS, IaaS, PaaS):

- Service name and vendor** - Exact name and company providing service



GSA CUI Phase 2 Documentation Checklist

- FedRAMP authorization status** - Authorized, not authorized, or pending
 - Data types** - Government data, CUI, PII, or other information types
 - Sensitivity level** - How sensitive is the data being transmitted
 - Direction of flow** - Inbound, outbound, or bidirectional
 - Authentication method** - How users connect (MFA required?)
 - Encryption methodology** - How data is encrypted in transit and at rest
 - Approval basis** - FedRAMP authorized, GSA risk approved, contract approved, etc.
 - Risk justification** - If non-FedRAMP, documented risk analysis and mitigation
-

SSPP Section 2 (System Environment): Critical Requirements

Section 2 defines your system boundary and operational environment[1]. This is fundamental to everything else.

Guidance for Section 2.0: System Environment

- Overall system description** - Clear narrative of what the system does and why
 - Architecture narrative** - Detailed explanation of how system components interact
 - Inventory reference** - References to attachment with complete system inventory
 - Data flows narrative** - Detailed description of how CUI and other data flows through system
 - Ports, protocols, services table** - Complete table with direction, source, destination, encryption status
 - Internal boundary enforcement** - How boundaries are enforced between network segments (VLANs, firewalls, etc.)
 - External integrations** - All connections to Internet, corporate network, external systems, APIs
 - Access control mechanisms** - All firewalls, ACLs, proxies, and cloud-based controls documented
 - Authentication point documentation** - Every login point (cloud console, jump host, database, application) described with MFA details
 - CUI data flow mapping** - Explicit trace of where CUI enters, moves through, and exits system
 - Admin access procedures** - Complete description of how administrators access the system, including all authentication hops
 - Third-party SaaS section** - If non-FedRAMP SaaS used: dedicated subsection with flow direction, auth, MFA, encryption, data contents
-



GSA CUI Phase 2 Documentation Checklist

Encryption documentation - All encryption protocols, ciphers, key management procedures documented

Deprecated technology check - Explicit verification that no TLS 1.0/1.1, SSL, or weak ciphers are present

CI/CD documentation - If applicable: documentation of continuous integration/deployment systems and code repositories

Ports, Protocols, and Services Table Requirements

Your ports/protocols table must include[1]:

Column	Required Data	Example
Direction	Inbound, Outbound, or Both	Inbound
Boundary Crossing	Y/N (does traffic cross system boundary?)	Y
Source	IP, DNS name, or resource type	10.0.1.0/24
Destination	IP, DNS name, or resource type	10.0.2.10
Ports	TCP or UDP with port numbers	tcp443, tcp22
Services	What services use these ports	HTTPS, SSH
Purpose	Why this traffic is needed	Admin access to jump host
Encrypted	Y/N and encryption protocol/cipher	Y - TLS 1.2, AES-256-GCM
Data Sensitivity	Sensitivity of data in traffic	CUI, PII, operational logs

Table 1: Ports, Protocols, and Services Table Format

Showstopper Requirements Documentation: Phase 2a Focus

In Phase 2a, GSA only reviews the 7 Showstopper requirements. Each must be fully implemented[1].

Access Control (03.01.02, 03.01.12)

- Access control policies documented** - Formal policies for all user roles and access types
- Access authorization procedures** - Process for granting, modifying, and revoking access



GSA CUI Phase 2 Documentation Checklist

- Architecture shows access points** - Diagram clearly shows all access control mechanisms
- Remote access detailed** - Complete description of remote access methodology, protocols, authentication
- Privileged access controlled** - Privileged commands only through authorized channels/jump hosts
- Jump host/bastion documented** - If used: detailed description of jump host architecture, access controls, MFA

Identification and Authentication (03.05.03)

- MFA inventory** - List of all locations requiring MFA (cloud consoles, jump hosts, databases, apps, APIs)
- MFA method documented** - Specific MFA method for each authentication point
- Privileged account MFA** - MFA enforced for ALL privileged accounts
- Non-privileged network access MFA** - MFA enforced for non-privileged accounts on network access
- Internet-accessible login MFA** - MFA enforced for all Internet-accessible logins
- Certificate-based auth protection** - If certificate auth used: cannot be downgraded to username/password only
- MFA method alignment** - All MFA methods evaluated against NIST SP 800-171 standards
- Customer responsibility statement** - If customers manage their own MFA: detailed guidance on how to implement

Risk Assessment (03.11.02)

- Vulnerability scanning program** - Documented vulnerability scanning schedule and procedures
- Scanning frequency defined** - Weekly OS scans, biweekly container scans, monthly web app scans documented
- Scan tools identified** - Specific vulnerability scanning tools listed
- Remediation procedures** - Process for remediating identified vulnerabilities
- Remediation timelines** - How quickly vulnerabilities are patched (within X days of discovery)
- CISA KEV process** - Documented procedure for CISA Known Exploited Vulnerabilities remediation
- EOL software documented** - Complete list of any End-of-Life software with risk mitigation plans



GSA CUI Phase 2 Documentation Checklist

- Scanning coverage** - All in-scope system components included in vulnerability scanning
- Quarterly reporting ready** - Process for compiling and submitting quarterly vulnerability reports

System and Communications Protection (03.13.01, 03.13.08, 03.13.11)

- Encryption in transit documented** - All CUI transmission encrypted with TLS 1.2+
- Encryption protocols detailed** - TLS version and cipher suites specified
- No deprecated protocols** - TLS 1.0, 1.1, SSL not present anywhere
- Encryption at rest documented** - All sensitive data (PII, authenticators, payment data) encrypted
- FIPS 140-2 validated modules** - Encryption modules are FIPS-approved and FIPS 140-2 validated
- FIPS module certificates** - FIPS 140-2 module certificate numbers provided
- Encryption key management** - How encryption keys are created, stored, distributed, signed
- Boundary protection documented** - All boundary protection mechanisms (firewalls, ACLs, proxies) described
- Ingress/egress protection** - Both inbound and outbound boundary protection detailed
- Network access controls** - Least-permissive network access controls documented
- Internal data flow encryption** - How internal CUI flows are encrypted between system components

System and Information Integrity (03.14.01)

- Patch management program** - Documented patch management process and schedule
- Flaw identification procedures** - How flaws are identified (automated scanning, vendor alerts, etc.)
- Update installation timeline** - How quickly patches are deployed after release
- Patching coverage** - All system components included in patch management
- Malware detection** - Antivirus/antimalware protection documented
- Unauthorized change detection** - Configuration management or file integrity monitoring explained
- EOL software status** - Any End-of-Life software clearly identified with mitigation strategy
- Patch testing process** - How patches are tested before production deployment



GSA CUI Phase 2 Documentation Checklist

System and Services Acquisition (03.16.02)

- System components inventory** - Complete list of all hardware, software, services with vendor and support status
 - Vendor assessment process** - How vendors are evaluated for security and compliance
 - Supply chain risk plan** - SCRM Plan document attached with vendor assessments
 - Risk mitigation documented** - For any unsupported components: documented risk evaluation and mitigation
 - Prohibited vendor check** - Verification that Kaspersky, Huawei, ZTE, Hikvision, Hytera, Dahua not used
 - Replacement plans** - For unsupported components: timeline for replacement or risk acceptance
- Third-party risk management** - How third-party vendors are monitored for security and compliance
- Vendor incident reporting** - How vendors are required to report incidents affecting your system
-

Security Requirement Narrative Quality Checklist

When you move to Phase 2b, each requirement narrative must answer: Who, What, Where, When, Why, How[1]

Requirement Narrative Structure

- Who** - Which roles/teams implement this requirement
- What** - Specific technical controls and tools used (don't generalize)
- Where** - Which systems/locations this applies to
- When** - When the requirement is enforced (always, on schedule, on event)
- Why** - How this requirement protects CUI (security context)
- How** - Detailed implementation methodology and tool usage

Quality Characteristics

- Clear and concise** - Professional language, no jargon without explanation
 - Specific, not generic** - Describe YOUR implementation, not boilerplate text
 - Consistent terminology** - Same terms used throughout for same concepts
 - Complete** - No blank areas, all required elements addressed
 - Responsive** - Directly answers the requirement, not tangential discussion
-



GSA CUI Phase 2 Documentation Checklist

- Component coverage** - Addresses all components in your system inventory
- Active voice** - "The Security Manager reviews logs" not "logs are reviewed"
- Consistent detail level** - Same level of detail across all requirement narratives
- No copied text** - No boilerplate copy-and-pasted across multiple requirements
- Technology referenced** - All technologies in narrative are shown in Section 2 architecture
- Customer responsibility identified** - If customer has role in implementation: clear Customer Responsibility statement
- POAM reference if needed** - For partially/planned implementations: POAM ID referenced with timeline
- Justification for NA** - Only mark "Not Applicable" with detailed justification if truly NA

What NOT to Do

- Avoid passive voice** - Don't write "Controls are implemented"; write "The Security Team implements controls using Tool X on Schedule Y"
- Don't restate requirement** - Describe specific implementation, not the requirement text
- Don't use boilerplate** - Each requirement should reflect your actual system
- Don't leave gaps** - Every component in your inventory should be mentioned
- Don't cite vaguely** - If citing documents, provide title, version, date, and section
- Don't use filler words** - Avoid "world-class," "user-friendly," "innovative," "such as"
- Don't mark NA without justification** - If you're not implementing something, explain why it doesn't apply

Privacy Documentation: PTA and PIA

Privacy Threshold Assessment (PTA) Checklist

- Submitted with Phase 2a** - PTA is required for all systems
- System description complete** - Clear description of system functionality and purpose
- PII determination** - Document whether system collects, processes, or stores PII
- PII types identified** - If PII is in scope: identify specific types (names, SSNs, addresses, etc.)
- PII collection method** - How and when PII is collected
- PII storage location** - Where PII is stored and for how long



GSA CUI Phase 2 Documentation Checklist

- PII sharing procedures** - How and with whom PII is shared
- PIA trigger** - Based on PTA responses: determination of whether PIA is needed

Privacy Impact Assessment (PIA) Checklist

- Submitted only if PTA indicates PII** - Conditional deliverable based on PTA outcome
- Privacy requirements identified** - Security and privacy controls for PII protection
- Data retention policy** - How long PII is retained and destruction procedures
- Access controls** - Who has access to PII and under what circumstances
- Transmission security** - How PII is protected in transit
- Individual notification** - If privacy incident occurs: how individuals are notified
- Approved by GSA Privacy Officer** - Submitted to privacy.office@gsa.gov for approval

Architecture Review Checklist Verification

The Security Architecture Review Checklist is a GSA-provided document you must complete^[1].

Completion Requirements

- All sections completed** - No blank responses
- Architectural elements verified** - Each item has been reviewed and response is accurate
- Consistency with diagram** - All checklist items align with your architecture diagram
- Consistency with inventory** - All checklist items align with your system inventory
- Showstopper items emphasized** - Special attention to Showstopper requirement checklist items
- Gaps identified** - Any known gaps documented with planned remediation
- Supporting evidence ready** - Documents referenced in checklist are available for review

Supply Chain Risk Management (SCRM) Plan

Required attachment to SSPP per NIST SP 800-161^[1].

SCRM Plan Checklist

- Vendor inventory** - Complete list of all vendors supplying components or services



GSA CUI Phase 2 Documentation Checklist

- Vendor assessment** - Security posture evaluation for each vendor
 - Risk evaluation** - Assessment of risks introduced by each third party
 - Risk mitigation** - Specific actions to address identified risks
 - Continuous monitoring** - How vendor security posture is tracked ongoing
 - Contract requirements** - Security clauses required in vendor contracts
 - Incident reporting** - Procedure for vendors to report security incidents
 - Supply chain flow** - Diagram or narrative showing how components flow from vendors into your system
-

Final Pre-Submission Checklist

Before submitting Phase 2a:

- All deliverables present** - SSPP Sections 1-2, Architecture, Showstoppers, Inventory, PTA/PIA, Review Checklist
 - Architecture reviewed by peers** - Have non-authors reviewed for clarity and completeness
 - Consistency verified** - Diagram matches SSPP matches Inventory matches Checklist
 - Prohibited vendors removed** - Kaspersky, Huawei, ZTE, Hikvision, Hytera, Dahua not present
 - Encryption verified** - All TLS 1.2+, FIPS modules documented with certificate numbers
 - MFA confirmed** - MFA implemented at all authentication points per requirements
 - Vulnerability scanning plan ready** - Documented scanning schedule for Phase 2b submission
 - EOL software addressed** - All End-of-Life components identified with mitigation plans
 - References complete** - All documents cited include title, version, date, section
 - Page count reasonable** - Sections 1-2 typically 30-50 pages depending on system complexity
 - Formatting consistent** - Professional document appearance, clear tables and diagrams
 - Typos and errors corrected** - Professional quality submission
 - Submission package complete** - All files included, naming conventions followed, ready to transmit
-
-



GSA CUI Phase 2 Documentation Checklist

Timeline Expectations

Understanding Phase 2 timing helps you plan realistically[1]:

Activity	Timeline
Phase 2a Preparation	4-6 weeks
Phase 2a Submission to GSA	1-2 days (depends on agency intake)
Phase 2a GSA Review	2-4 weeks
Phase 2a Feedback and Rework	1-4 weeks (if issues found)
Phase 2a Approval by GSA CISO	1 week (after successful review)
Phase 2b Preparation	4-8 weeks
Phase 2b GSA Review	4-6 weeks
Phase 2b Approval by GSA CISO	1 week
Total Phase 2	4-6 months minimum

Table 2: Phase 2 Timeline Expectations

Savings Opportunity: Getting Phase 2a approved on first submission saves 4-8 weeks. Use this checklist to avoid common rework causes[1].

The Difference Between Approved and Rejected Phase 2 Submissions

Approved Phase 2a Packages Have These Characteristics

- Clear, detailed architecture with prominent system boundary
- Complete system inventory with all components mapped to diagram
- Specific Showstopper requirement implementations describing system-specific controls
- Documented MFA at all authentication points
- Verified encryption standards (TLS 1.2+, FIPS modules with certificate numbers)
- Vulnerability scanning schedule with specific tools and frequencies
- Supply chain risk management addressing all vendors
- Consistent terminology and detail level across all documents
- No blank areas; all questions answered with specific information



GSA CUI Phase 2 Documentation Checklist

- Evidence of pre-submission review and quality verification

Rejected Phase 2a Packages Have These Problems

- Architecture diagram with insufficient detail or "black box" components
- Missing authentication point identification or MFA documentation
- Generic, boilerplate requirement narratives not specific to their system
- Incomplete or missing system inventory items
- Unverified encryption status or use of deprecated protocols
- No documented vulnerability scanning plan
- Missing or incomplete SCRM plan
- Inconsistencies between diagram, inventory, and SSPP narrative
- Blank areas in checklist items or vague responses
- Lack of evidence of review or quality verification before submission

Key Takeaways

1. **Phase 2a is your first opportunity to succeed** - Get it right on first submission[1]
2. **Architecture is everything** - Your diagram determines assessment scope and complexity[1]
3. **Specificity matters** - GSA wants your implementation, not generic boilerplate[1]
4. **Consistency wins approval** - Diagram, inventory, and narrative must align perfectly[1]
5. **Documentation details** - Use this checklist to audit before submission[1]
6. **Showstoppers are non-negotiable** - All 7 must be fully implemented[1]
7. **Quality saves weeks** - First-submission approval can save 4-8 weeks of total timeline[1]

References

[1] U.S. General Services Administration. (2026). CIO-IT Security-21-112, Revision 1: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations. Retrieved from <https://www.gsa.gov/cdnstatic/CIO-IT Security-21-112 Rev 1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Process.pdf>