



The Federal Contractor's Guide to GSA CUI Authorization

Protecting Controlled Unclassified Information Under CIO-IT Security-21-112, Revision 1

Executive Summary

The GSA released an updated procedural guide for protecting Controlled Unclassified Information (CUI) in nonfederal systems on January 5, 2026. This revision, CIO-IT Security-21-112 Revision 1, introduces stricter requirements aligned with NIST SP 800-171r3 and 800-172r3 Draft[1].

For federal contractors handling CUI, the implications are significant: outdated system architectures will fail authorization, Phase 2 documentation gaps are the leading cause of assessment delays, and 7 specific "Showstopper" requirements can disqualify your system entirely if not fully implemented[1].

The reality: Contractors who understand these requirements upfront save 8-12 weeks of rework and avoid assessment failures.

What Changed in CIO-IT Security-21-112, Revision 1

Key Updates from the Original Guide

The January 2026 revision introduces critical changes that directly impact authorization timelines[1]:

- **Alignment to NIST 800-171r3 and 800-172r3 Draft** - Stricter security posture requirements across all system components
- **Mandatory Supply Chain Risk Management Documentation** - New requirement for vendor assessment and third-party risk management plans
- **Enhanced Boundary Definition and Data Flow Standards** - More detailed architecture documentation with specific port/protocol requirements
- **Specific MFA, Encryption, and Remote Access Requirements** - Clear standards for authentication mechanisms and secure admin access
- **Showstopper Requirements Codified in Appendix C** - Seven security requirements that will block authorization if not fully implemented

Why This Matters Now

Most federal contractors are operating under outdated compliance assumptions. Systems that passed authorization under the original guide may not meet the new standards. This creates two critical risks[1]:



The Federal Contractor's Guide to GSA CUI Authorization

1. **Assessment Failure Risk** - Your current system architecture may fail GSA review
 2. **Timeline Risk** - Discovering gaps during assessment adds 8-12 weeks to your authorization process
-

The Showstopper Requirements

These requirements are non-negotiable. If any are not fully implemented, GSA will not authorize your system[1][2].

1. Access Control (Requirements 03.01.02, 03.01.12)

Requirement Title: Access Enforcement & Remote Access

What GSA Reviews:

- Approved authorizations for logical access to CUI and system resources
- Usage restrictions, configuration requirements, and connection requirements for remote system access
- Remote access routed through authorized and managed access control points
- Privileged command execution only through authorized channels

Critical Documentation Needs:

- Complete access control policies for all user roles
- Architecture diagram showing all access control mechanisms (firewalls, ACLs, proxies)
- Remote access methodology with detailed authentication flows
- Authorization procedures for each type of system access

2. Identification and Authentication (Requirement 03.05.03)

Requirement Title: Multi-Factor Authentication (MFA) Implementation

What GSA Reviews:

- MFA enforcement for **all privileged accounts**
 - MFA enforcement for **all non-privileged accounts with network access**
 - MFA enforcement for **all Internet-accessible logins**
 - No downgrade from certificate-based authentication to username/password only
-



The Federal Contractor's Guide to GSA CUI Authorization

Critical Documentation Needs:

- Inventory of all authentication points (cloud consoles, jump hosts, databases, applications, APIs)
- MFA method validation against NIST SP 800-171 standards
- Proof that MFA is enforced at user object level, not device level
- Customer responsibility statements if customers manage authentication

3. Risk Assessment (Requirement 03.11.02)

Requirement Title: Vulnerability Monitoring and Scanning

What GSA Reviews:

- Documented vulnerability monitoring at defined frequency
- Vulnerability remediation within documented timeframes
- Remediation procedures for new vulnerabilities
- System inventory of all components requiring scanning

Critical Documentation Needs:

- Vulnerability scanning schedule (minimum: weekly authenticated OS scans, biweekly container scans, monthly web app scans)
- Scanning tools and methodologies
- CISA Known Exploited Vulnerabilities (KEV) remediation plan
- End-of-Life (EOL) software inventory and risk mitigation strategies
- Quarterly and annual scanning deliverables

4. System and Communications Protection (Requirements 03.13.01, 03.13.08, 03.13.11)

Requirement Title: Boundary Protection, Encryption, and Cryptographic Protection

What GSA Reviews:

- **Boundary Protection:** External and internal interface monitoring and control
- **Encryption in Transit:** All CUI transmission encrypted with TLS 1.2 or higher
- **Encryption at Rest:** Sensitive data (PII, payment card data, authenticators) encrypted with FIPS-validated modules



The Federal Contractor's Guide to GSA CUI Authorization

- Encryption ciphers and key management procedures
- Prohibition of deprecated encryption protocols (anything below TLS 1.2)

Critical Documentation Needs:

- System architecture showing all boundary protection devices
- Data flow diagram identifying all encrypted vs. unencrypted flows
- Encryption methodology and algorithm documentation
- FIPS 140-2 validated module certificate numbers
- Proof of TLS 1.2+ implementation on all connections

5. System and Information Integrity (Requirement 03.14.01)

Requirement Title: Flaw Remediation and Patch Management

What GSA Reviews:

- System flaw identification and reporting procedures
- Security-relevant software and firmware update installation timelines
- Patch management coverage for all components
- Proof that outdated/deprecated software is not present

Critical Documentation Needs:

- Patch management procedures and tools
- Update installation timelines (within defined organization-determined days)
- Inventory of all software components and support status
- EOL software justification if any is retained
- Malware detection and unauthorized change detection mechanisms

6. System and Services Acquisition (Requirement 03.16.02)

Requirement Title: Unsupported System Components and Vendor Risk Management

What GSA Reviews:

- Replacement plans for unsupported system components
- Risk mitigation for components that cannot be replaced
- Vendor assessment and supply chain risk management
- Prohibition of technology from banned vendors (Kaspersky Lab, Huawei, ZTE, Hikvision, Hytera, Dahua)



The Federal Contractor's Guide to GSA CUI Authorization

Critical Documentation Needs:

- Complete system component inventory with vendor and support status
 - Supply Chain Risk Management (SCRM) Plan aligned with NIST SP 800-161
 - Vendor assessment procedures and results
 - Risk acceptance documentation for any retained unsupported components
-

Phase 2 Documentation: The Timeline Killer

Phase 2 is where most contractors experience delays. This phase requires detailed system documentation that must pass GSA review before you can proceed to assessment[1][3].

Phase 2 Deliverables Checklist

All of these documents must be completed and approved before Phase 3 (Assessment) can begin:

- **Privacy Threshold Assessment (PTA)** - Required for all systems; determines if Privacy Impact Assessment (PIA) is needed
- **Privacy Impact Assessment (PIA)** - Conditional, based on PTA outcome; required if PII is in scope
- **System Security and Privacy Plan (SSPP) - Sections 1 & 2 (Initial Submission)** - Architecture focus, Showstopper requirements only
- **System Security and Privacy Plan (SSPP) - Complete Submission** - All security and privacy requirements documented
- **Architecture Diagram and Boundary Definition** - Detailed, comprehensive system boundary
- **Integrated Inventory, Leveraged and External Services Workbook** - Complete asset and service inventory
- **Supply Chain Risk Management Plan** - Vendor assessment and third-party risk documentation
- **Ports, Protocols, and Services Tables** - All network flows documented with encryption status
- **Security Architecture Review Checklist** - Verification that all architectural elements meet requirements

What GSA Reviewers Look for in Phase 2

Architecture Diagram Requirements (Will cause rejection if missing)[3]:

1. Prominent border around all system components and services in the boundary
-



The Federal Contractor's Guide to GSA CUI Authorization

2. Separate borders for protected enclaves, subnets, and DMZs
3. All assets, services, devices, and software - both physical and virtual
4. COOP/DR site integrations and test/development environments if in scope
5. All components that handle, process, or store CUI or metadata
6. Integration points with external systems, VPNs, and APIs clearly identified
7. Source/destination, ports/protocols, and encryption status on all flows
8. Access control mechanisms (firewalls, ACLs, proxies) fully documented
9. Ports/protocols/services tables with direction (inbound/outbound/both)
10. FedRAMP authorized vs. non-FedRAMP services clearly identified
11. All authentication points clearly depicted with MFA indicators
12. Prohibited vendor technology explicitly excluded

Data Flow Documentation Requirements:

- Narrative descriptions of all data flows (how CUI enters, moves through, and exits the system)
- Diagrams showing data flows in both narrative and visual forms
- Documentation of all CI/CD systems and code repositories if applicable
- Identification of which data flows are encrypted and which are not
- For unencrypted flows: description of data contents, sensitivity level, and access controls

SSPP Requirement Narrative Requirements:

Each requirement narrative must answer: **Who, What, Where, When, Why, and How**[1][3]

- **Who** - Which roles/teams implement this requirement
- **What** - Specific technical controls and tools used
- **Where** - Which systems/locations this applies to
- **When** - When the requirement is enforced (always, on schedule, on event)
- **Why** - How this requirement protects CUI
- **How** - Detailed implementation methodology and tool usage

Critical Requirement Implementation Guidance:

- Do NOT simply restate the requirement; describe your **specific implementation**
- Ensure every technology mentioned in Section 3 is documented in Section 2 architecture



The Federal Contractor's Guide to GSA CUI Authorization

- Include Customer Responsibility statements for shared implementation areas
- For partially or planned implementations, include POAM reference and timeline
- Ensure consistency across all requirement narratives

Architecture Diagram Critical Elements

Your system boundary diagram is the foundation of your entire authorization package. GSA reviewers will scrutinize it against your SSPP and inventory. Missing elements will cause rejection and rework[3].

Authorization Boundary Diagram (ABD) Essentials

Diagram Element	GSA Review Criteria
System Boundary	Prominent border around ALL components in scope
Component Detail	Every asset, device, service (physical and virtual)
Enclaves & Subnets	Separate borders for protected enclaves, subnets, DMZs
External Connections	All integrations with external systems, SaaS, APIs clearly shown
Data Flows	Source/destination, ports/protocols, encryption status
Access Controls	All firewalls, ACLs, proxies, and network controls depicted
Authentication Points	Every place users authenticate (cloud console, jump host, app, API)
Leveraged Services	FedRAMP vs. non-FedRAMP services differentiated
Monitoring Tools	SIEM, vulnerability scanners, antivirus, IDS/IPS included

Table 1: Authorization Boundary Diagram Review Elements

Common Reasons for Phase 2 Rejection

- Insufficient detail (components as "black boxes" without internal flows)
- Missing authentication point identification
- Failure to show CUI data flows clearly
- Missing external service documentation



The Federal Contractor's Guide to GSA CUI Authorization

- 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 present in diagram

Critical Security Implementation Guidance

MFA Implementation Standards

Per NIST SP 800-171r3 and GSA guidance, MFA must be implemented at these critical points[1][2]:

- **All privileged account access** (administrative consoles, databases, cloud platforms)
- **All non-privileged network access** (from non-trusted networks)
- **All Internet-accessible logins** (any portal accessible from the internet)
- **All external service access** (SaaS platforms, cloud consoles, APIs)
- **Secure admin access** (jump hosts, bastion servers, remote administration tools)

MFA Methods Evaluated by GSA:

- Time-based One-Time Password (TOTP) - Approved, phishing resistant
- Hardware tokens - Approved, highest security
- Certificate-based authentication - Approved for privileged access
- SMS/Email OTP - Restricted, susceptible to interception
- Security questions - NOT approved

MFA Configuration Requirements:

- Enforce at **user object level**, not device level
- Do NOT allow single sign-on (SSO) pass-through credentials
- Require manual logon prompt for jump hosts/bastion servers
- Certificate-based authentication cannot be downgraded to username/password

Encryption Standards

At Rest (for CUI, PII, authenticators, payment card data):



The Federal Contractor's Guide to GSA CUI Authorization

- FIPS-approved ciphers (AES-256-GCM or AES-256-CBC minimum)
- FIPS 140-2 validated encryption modules
- Acceptable at file, database table, column, or field level
- Application-level encryption or tokenization acceptable
- Provide FIPS 140-2 module certificate numbers

In Transit (all CUI transmission):

- TLS 1.2 or higher (TLS 1.3 preferred)
- Deprecated protocols explicitly prohibited:
 - TLS 1.0, TLS 1.1
 - SSL 2.0, SSL 3.0
 - Any weak cipher suites
- Cryptographic algorithm validation per NIST standards

Vulnerability Scanning Requirements

Component Type	Scan Frequency	Authentication
Operating System (OS)	Weekly	Authenticated
Container Images	Biweekly	Authenticated
Container Configuration	Biweekly	Authenticated
Database	Biweekly	Authenticated
Web Applications	Monthly	Authenticated (private), Unauthenticated (public)

Table 2: Vulnerability Scanning Frequency Requirements

Critical Requirements:

- Weekly authenticated scans for major OS systems (Windows, Unix, Linux)
- CISA Known Exploited Vulnerabilities (KEV) must be remediated
- Residual KEV vulnerabilities are considered Showstopper conditions
- EOL (End-of-Life) software must have documented risk mitigation
- Residual EOL software vulnerabilities are Showstopper conditions



The Federal Contractor's Guide to GSA CUI Authorization

- Quarterly scanning reports due one month before quarter end

Remote Access Security Standards

Secure remote administration (jump hosts/bastion servers) must follow these GSA-approved guidelines[1]:

- MFA required for access to jump host
- Non-persistent, unique sessions on logon
- Jump box access restricted via ACL to defined IPs/subnets/VLANs
- Jump box NOT publicly accessible (corporate network or VPN only)
- If VPN used: MFA on VPN client (phishing-resistant OTP required)
- VPN must NOT allow split tunneling
- Dedicated service accounts tied to corporate or boundary Active Directory
- Credentials NOT passed through SSO; manual logon required
- MFA enforced at user object level
- All connections use encrypted communication (TLS 1.2+)
- New connection launched from jump box, not administrator's workstation

External Services and FedRAMP Requirement

If your system leverages external services (SaaS, IaaS, PaaS), GSA has specific approval criteria[1]:

FedRAMP Authorization Requirement

- **FedRAMP-authorized IaaS services:** May be used with documented approval
- **FedRAMP-authorized SaaS services:** Preferred for all external integrations
- **Non-FedRAMP services:** Will be evaluated by GSA on a risk basis
- **Prohibited services:** Must identify alternative or justify risk acceptance

External Service Documentation Requirements

For each external service, document:

- Service name and FedRAMP authorization status
- Data types flowing to/from service (government vs. non-government)



The Federal Contractor's Guide to GSA CUI Authorization

- Sensitivity level of data
- Direction of flow (inbound, outbound, or both)
- Encryption methodology
- Authentication method (must include MFA if CUI is involved)
- Frequency and volume of data transfer
- Risk acceptance if non-FedRAMP authorized

Prohibited Vendor Technology

Per Section 1634 of Public Law 115-91 and FAR 52.204-25, these companies and their subsidiaries/affiliates are prohibited[1]:

- Kaspersky Lab
- Huawei
- ZTE
- Hikvision
- Hytera
- Dahua

Verification Required: Your SSPP must confirm that prohibited vendor technology is not present in your system architecture or any external services.

Supply Chain Risk Management (SCRM) Plan

A SCRM plan is a required attachment to your SSPP[1][3]. This plan must address vendor assessment and third-party risk management aligned with NIST SP 800-161.

SCRM Plan Requirements

- **Vendor identification** - All vendors supplying components or services
- **Vendor assessment** - Security posture evaluation of each vendor
- **Risk evaluation** - Assessment of risks introduced by third parties
- **Risk mitigation** - Specific actions to address identified risks
- **Continuous monitoring** - How you will track vendor security posture ongoing
- **Contract requirements** - Security clauses mandated in vendor contracts
- **Incident reporting** - Procedure for vendors to report incidents affecting your system



The Federal Contractor's Guide to GSA CUI Authorization

Self-Assessment Recommendation

GSA encourages vendors to perform self-assessment against all security and privacy requirements in Appendix C of this guide. Identify and document any known gaps in your SSPP, along with detailed remediation plans[1].

Continuous Monitoring and Authorization Timeline

After GSA authorization, your compliance obligations don't end. Continuous monitoring is required[1]:

Quarterly Deliverables (Due Monthly)

- Updated vulnerability scanning reports
- Security event summaries from your SIEM
- Changes to system configuration or components
- Patch management status

Annual Deliverables (Due 2 months before fiscal year end, September 30)

- Comprehensive system security assessment
- Updated SCRM plan evaluation
- Annual vulnerability management summary
- Incident summary (if any incidents occurred)

Three-Year Deliverable

- Comprehensive privacy and security assessment (for systems with PIA)

Major Changes Requiring Pre-Notification

Must notify GSA ISSO, ISSM, and Contracting Officer BEFORE implementation:

- Changes to CUI data types or retention
 - Changes to encryption protecting CUI data
 - System re-hosting or re-platforming
 - Addition of new external services handling CUI
 - Removal of security components
 - Removal of MFA requirements
-
-



The Federal Contractor's Guide to GSA CUI Authorization

Timeline Expectations

Understanding the GSA authorization process timeline helps you plan more effectively[1]:

Phase	Timeline
Phase 1: Prepare	4-8 weeks
Phase 2a: Initial SSPP (Sections 1-2 + Showstoppers)	4-6 weeks submission; 2-4 weeks GSA review
Phase 2b: Complete SSPP	4-8 weeks submission; 4-6 weeks GSA review
Phase 3: Assessment	6-12 weeks (including remediation and POAM closure)
Phase 4: Authorization	2-4 weeks GSA CISO review
Total	4-6 months minimum

Table 3: GSA CUI Authorization Timeline

Critical Success Factor: Contractors who get Phase 2 documentation approved on first submission save 8-12 weeks of total timeline.

Key Takeaways for Federal Contractors

1. **The seven Showstopper requirements are non-negotiable** - Full implementation is required before authorization is possible[1][2]
2. **Architecture documentation is your foundation** - Detailed system boundary diagrams and data flow documentation directly impact assessment success
3. **Phase 2 is where delays happen** - Documentation gaps are the leading cause of assessment rework and timeline delays[1]
4. **MFA is everywhere** - Every authentication point requires multi-factor authentication implementation
5. **Encryption standards are strict** - TLS 1.2+, FIPS-validated modules, and documented key management are non-negotiable
6. **NIST 800-171r3 is your baseline** - All security requirements map to specific NIST controls with defined assessment procedures



The Federal Contractor's Guide to GSA CUI Authorization

7. **Vendor management is mandatory** - Supply chain risk management plans must be comprehensive and regularly updated
8. **Continuous monitoring never stops** - Authorization is not the end; quarterly and annual reporting continues throughout the contract

Next Steps

To accelerate your CUI authorization process:

1. **Audit your current system architecture** against the Showstopper requirements
2. **Identify gaps in MFA implementation**, encryption standards, and vulnerability scanning
3. **Develop your SSPP using GSA templates** - Invest in quality documentation upfront
4. **Engage a GSA-approved 3PAO assessor early** - Get feedback on your architecture before formal assessment
5. **Build your supply chain risk management plan** - Document vendor assessments and risk mitigation

Organizations that follow these steps reduce their authorization timeline by 8-12 weeks and significantly increase the probability of first-submission approval.

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>

[2] National Institute of Standards and Technology. (2024). NIST SP 800-171 Revision 3: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. <https://csrc.nist.gov/publications/detail/sp/800-171/rev-3>

[3] U.S. General Services Administration. (2026). Appendix D: Boundary Diagram Guidance. In CIO-IT Security-21-112, Revision 1. GSA.