



The Showstopper Requirements

Critical Security Controls That Block GSA CUI Authorization

If your system doesn't fully implement these, GSA will not authorize it—period.

This guide breaks down exactly what each Showstopper requirement means, what GSA reviewers are looking for, and what "fully implemented" actually looks like according to CIO-IT Security-21-112, Revision 1[1].

Use this as your technical reference during system architecture design, implementation, and documentation phases.

Overview: The Six Showstopper Categories

GSA has identified six security categories as "Showstopper" requirements. If any single requirement within these categories is not fully implemented, your system fails authorization[1][2].

Category	Requirements	Core Focus
Access Control	03.01.02, 03.01.12	User/system authentication and access enforcement
Identification & Authentication	03.05.03	Multi-factor authentication at all critical points
Risk Assessment	03.11.02	Vulnerability management and threat identification
System & Communications Protection	03.13.01, 03.13.08, 03.13.11	Encryption, boundary protection, network controls
System & Information Integrity	03.14.01	Patch management and flaw remediation
System & Services Acquisition	03.16.02	Unsupported components and vendor management

Table 1: The Six Showstopper Categories

Showstopper #1: Access Control (03.01.02, 03.01.12)

Requirement Title

Enforce Access Controls and Remote Access Security

What GSA Is Checking

Requirement 03.01.02 - Enforce Access:



The Showstopper Requirements

- Logical access to the system and CUI is limited to authorized users, processes, and devices
- Access enforcement mechanisms are in place and documented
- Access is granted based on need-to-know and role-based principles
- Access reviews are performed at defined intervals

Requirement 03.01.12 - Remote Access:

- Remote access to the system is controlled and monitored
- Remote connections use secure protocols and authentication
- Remote access is routed through approved access control points (jump hosts/bastion servers)
- Privileged command execution only through authorized channels[1]

What "Fully Implemented" Means

Your architecture must include:

- **Formal access control policy** - Written policy defining roles, access types, and authorization procedures
- **Access control mechanisms** - Technical controls that enforce access decisions (firewalls, ACLs, proxy servers, IAM systems)
- **Multiple layers of access control** - Authentication, authorization, and auditing at each tier
- **Complete audit logging** - All access requests and approvals logged for review
- **Jump host/bastion architecture** - Privileged access routed through dedicated, hardened jump servers
- **Jump host isolation** - Jump host only accessible from approved networks/IPs
- **Session recording** - All privileged sessions recorded and retained
- **Access reviews** - Formal quarterly or annual access reviews documented
- **Access revocation procedures** - Documented process for removing access immediately when needed
- **Separation of duties** - Access approval separate from access implementation
- **Internet accessibility restrictions** - Privileged access NOT directly accessible from Internet
- **Encryption of remote sessions** - All remote access encrypted (SSH, TLS 1.2+, not Telnet/HTTP)

Implementation Example: Jump Host Architecture

A compliant remote access architecture typically includes:



The Showstopper Requirements

1. **VPN Gateway** - Users connect to corporate VPN with MFA (Okta, Duo, etc.)
2. **Jump Host** - Hardened Linux/Windows server accessible only from corporate network
3. **Target Systems** - Administrators SSH/RDP to target systems through jump host

MFA Flow: VPN MFA → SSH to Jump Host → RDP to Target Server

Key Detail: Each hop requires separate authentication. Credentials are NOT passed through; new authentication occurs at each step.

GSA Review Checklist for 03.01.02 / 03.01.12

- Does the architecture diagram show all access control mechanisms?
- Are jump hosts/bastion servers prominently depicted?
- Are all authentication points identified with MFA indicators?
- Is the access control policy referenced and available?
- Does the SSPP narrative explain access control enforcement for each user role?
- Is remote access methodology fully documented?
- Are access logging and review procedures documented?
- Is there evidence that Internet-accessible login points are NOT used for privileged access?
- Are encrypted protocols (SSH, TLS 1.2+) used, not unencrypted (Telnet, HTTP)?
- Is session recording capability present for privileged access?

Common Implementation Gaps

- **Black box jump host** - Jump host shown but internal access controls not explained
- **Missing MFA documentation** - Architecture shows jump host but MFA not mentioned
- **Unencrypted remote access** - RDP/SSH without encryption or over unencrypted networks
- **Direct Internet access to privileged systems** - Privileged interfaces directly exposed to Internet instead of through jump host
- **Shared credentials** - Multiple administrators sharing same username/password for privileged access
- **No session recording** - Privileged access not logged or recorded for audit

Showstopper #2: Identification and Authentication (03.05.03)



The Showstopper Requirements

Requirement Title

Use Multi-Factor Authentication for All Critical Access Points

What GSA Is Checking

Multi-factor authentication must be implemented at three critical points[1]:

1. **Privileged account access** - ALL administrators accessing systems
2. **Non-privileged network access** - Non-admin users accessing from outside trusted networks
3. **Internet-accessible logins** - ANY login available from the public Internet

What "Fully Implemented" Means

MFA must protect:

- **Cloud console access** - AWS, Azure, GCP management consoles
- **Jump host/bastion servers** - Any administrator jump box
- **Database administrative consoles** - Direct database admin access
- **Virtualization platforms** - vSphere, Hyper-V admin interfaces
- **Directory services** - Active Directory admin access
- **Application management portals** - Any admin interface to applications
- **API gateway/management** - Admin endpoints for API management
- **Remote desktop protocol (RDP)** - Windows RDP admin access
- **Secure shell (SSH)** - Linux/Unix SSH admin access
- **Web portals with Internet access** - Any web portal accessible from public Internet
- **Customer-facing applications** - If users access CUI through application: MFA for users
- **Service account management** - Where applicable: MFA enforcement for service accounts with privileged access

Approved MFA Methods (Per NIST SP 800-171)

Phishing-Resistant (Preferred):

- Hardware tokens (FIDO2 security keys)
- PIV cards (Personal Identity Verification)
- Certificate-based authentication

Acceptable:



The Showstopper Requirements

- Time-based One-Time Password (TOTP) - Google Authenticator, Authy, Microsoft Authenticator
- Push notifications to registered device - Okta Push, Duo Push
- Voice/SMS OTP - Less preferred but acceptable (susceptible to interception)

NOT Acceptable:

- Security questions alone
- SMS/Email OTP alone (must be paired with another factor)
- Single sign-on (SSO) pass-through without separate MFA prompt

What "Fully Implemented" Does NOT Mean

- × Enforcing MFA at device level but allowing credential pass-through to jump host
- × Using SSO to bypass MFA on jump host access
- × Implementing MFA on user workstations but not on system access
- × Requiring MFA once per day but allowing unlimited access after initial authentication
- × Allowing downgrade from certificate-based auth to password-only authentication
- × Using only SMS OTP without a second factor
- × Exempting service accounts from MFA requirements

Implementation Example: MFA for Cloud Console Access

Compliant AWS Console Access:

1. User navigates to AWS login page
2. Enters username and password
3. AWS prompts for MFA code
4. User enters TOTP from Authenticator app
5. User gains access to AWS console

Authentication sequence: Something you know (password) + Something you have (authenticator app) = MFA

Non-Compliant Example:

- User logs in with SSO (single sign-on)
- SSO provides credentials that work on AWS
- User never prompted for second factor
- User can access AWS console
- This is NOT MFA; it's SSO pass-through



The Showstopper Requirements

GSA Review Checklist for 03.05.03

- Is MFA implemented at all privileged account access points?
- Is MFA implemented for all non-privileged network access (from untrusted networks)?
- Is MFA implemented for all Internet-accessible logins?
- Are all MFA methods documented and aligned with NIST SP 800-171?
- Are approved MFA methods used (no security questions alone, no SMS-only)?
- Are MFA implementation details provided (which tool, which authentication points)?
- Is MFA enforced at user object level, not device level?
- Are service accounts with privileged access subject to MFA?
- If certificate-based auth used: is downgrade to password-only prevented?
- Are customer responsibility statements provided where customers manage MFA?
- Is there evidence of MFA implementation (screenshots, configuration exports, policy documentation)?
- Is MFA available in all geographic regions/availability zones where system operates?

Common Implementation Gaps

- **Incomplete MFA coverage** - MFA at some access points but not all
- **Unapproved MFA methods** - Using security questions, SMS-only, or other non-NIST-approved methods
- **SSO bypass** - Single sign-on passes credentials without second factor
- **Device-level enforcement** - Enforcing MFA on workstation but not system access
- **Service account exemption** - Excluding service accounts with privileged access from MFA
- **No customer guidance** - If customers manage their own access: not providing clear MFA configuration instructions
- **Certificate downgrade** - Allowing certificate-based auth to downgrade to password-only

Showstopper #3: Risk Assessment (03.11.02)

Requirement Title

Identify, Document, and Remediate Vulnerabilities

What GSA Is Checking

Your organization must have a vulnerability management program that[1]:



The Showstopper Requirements

1. **Identifies vulnerabilities** through regular scanning
2. **Evaluates vulnerability risk** using documented criteria
3. **Remediates vulnerabilities** according to defined timelines
4. **Tracks CISA Known Exploited Vulnerabilities (KEV)** as highest priority
5. **Prevents deployment of vulnerable software** through scanning processes
6. **Removes End-of-Life (EOL) software** or documents risk mitigation

What "Fully Implemented" Means

Vulnerability Management Program Components:

- **Automated vulnerability scanning** - Regular, scheduled scans of all system components
- **Operating system scanning** - Weekly authenticated scans of all servers (Windows, Linux, Unix)
- **Container image scanning** - Biweekly scans of all container images in use
- **Database vulnerability scanning** - Biweekly scans of database systems
- **Web application scanning** - Monthly scans of web applications (authenticated for internal, unauthenticated for public-facing)
- **Network vulnerability scanning** - Regular scans identifying open ports, services, protocols
- **Vulnerability scanning tools** - Multiple vendors (Nessus, Qualys, Rapid7, etc.) or approved equivalent
- **Remediation procedures** - Documented process for addressing identified vulnerabilities
- **Remediation timelines** - Security vulnerabilities patched within X days (typically 14-30 days depending on severity)
- **Critical patches** - Vulnerabilities with CISA KEV status remediated within defined urgent timeline
- **Scanning coverage verification** - All in-scope components confirmed to be covered by scanning
- **Scan result analysis** - Regular review and remediation of identified vulnerabilities
- **False positive process** - Documented procedure for investigating and dismissing false positives
- **EOL component tracking** - Inventory of any End-of-Life software with documented risk mitigation
- **CISA Binding Operational Directive (BOD) compliance** - Adherence to CISA BOD timelines

Vulnerability Scanning Frequency Requirements

Component Type	Frequency	Authentication
Operating Systems	Weekly	Authenticated
Containers	Biweekly	Authenticated
Container Config	Biweekly	Authenticated
Databases	Biweekly	Authenticated
Web Applications	Monthly	Auth (internal), Unauth (public)
Network (infrastructure)	Monthly to Quarterly	Unauthenticated

Table 2: GSA Vulnerability Scanning Frequency Requirements

CISA Known Exploited Vulnerabilities (KEV) Treatment

GSA considers residual CISA KEV vulnerabilities that cannot be corrected as a Showstopper condition[1].

Your obligation:

- Monitor CISA KEV catalog (<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>)
- Identify if any KEV affects your systems
- Remediate KEV on urgent timeline (per CISA BOD requirements)
- If KEV cannot be remediated: documented risk evaluation and GSA CISO approval

CISA BOD Timelines (Current):

- **2-7 days:** Critical CISA-mandated directives
- **30 days:** Known Exploited Vulnerability (KEV) remediation
- **Ongoing:** Known Exploited Vulnerabilities catalog monitoring

End-of-Life (EOL) Software Treatment

If your system contains End-of-Life software (no longer supported by vendor)[1]:

- GSA will conduct risk evaluation
- If residual EOL software vulnerabilities exist that cannot be corrected: Showstopper condition
- You must either:
 - Replace the EOL component, OR
 - Document risk evaluation and receive GSA CISO approval, OR
 - Implement compensating controls



The Showstopper Requirements

Implementation Example: Vulnerability Management Program

Weekly OS Scan Execution:

1. Sunday night: Automated Nessus scan of all Windows/Linux servers
2. Monday: Scan results reviewed by Security Team
3. Tuesday: Vulnerabilities categorized by severity
4. Wednesday-Thursday: Remediation begins (patches, configuration changes)
5. Friday: Verification scans confirm remediation
6. Monthly: Summary report compiled for stakeholders

Critical Vulnerability Response:

1. CISA KEV identified by automated scanning
2. Incident response triggered within 2 hours
3. Emergency change control initiated
4. Patch/workaround deployed within CISA deadline
5. Verification scan confirms remediation

GSA Review Checklist for 03.11.02

- Is vulnerability scanning performed at required frequencies?
- Are authenticated scans performed on OS, databases, containers?
- Are scanning tools identified and appropriate for component types?
- Is there documented evidence of regular scan execution (scan reports)?
- Are vulnerability remediation procedures documented?
- Are remediation timelines defined (security vuln within X days)?
- Is CISA KEV process documented?
- Are residual CISA KEV vulnerabilities absent, or is GSA approval obtained?
- Is EOL software absent, or is risk mitigation documented and approved?
- Are scanning results retained for audit purposes (past 12+ months)?
- Is remediation evidence available (patch deployment records, configuration changes)?
- Are scanning results reviewed and acted upon, not just collected?

Common Implementation Gaps

- **Infrequent scanning** - Scanning monthly instead of weekly for critical OS systems
- **Unauthenticated scans only** - Missing authenticated scans that detect more vulnerabilities



The Showstopper Requirements

- **Scanning without remediation** - Running scans but not addressing findings
 - **Slow remediation** - Vulnerabilities taking 90+ days to patch
 - **No CISA KEV tracking** - Not monitoring CISA KEV catalog for system-specific vulnerabilities
 - **Unaddressed CISA KEV** - Residual CISA KEV vulnerabilities with no GSA approval
 - **No EOL software inventory** - EOL components present without documented risk mitigation
 - **Scanning tools not identified** - "Scanning is performed" without specifying tool or methodology
 - **No historical data** - Scanning results not retained for audit trail
-

Showstopper #4: System and Communications Protection (03.13.01, 03.13.08, 03.13.11)

Requirement Title

Encrypt Data in Transit and at Rest; Implement Boundary Protection

What GSA Is Checking

Three critical requirements in this category[1]:

03.13.01 - Boundary Protection:

- All external and internal system boundaries are monitored and controlled
- Data flows across system boundaries are enforced through defined mechanisms
- Ingress/egress filtering is in place

03.13.08 - Cryptographic Protection (In Transit):

- CUI transmitted across system boundaries or networks is encrypted
- Encryption uses approved cryptographic standards and algorithms
- Encryption strength is commensurate with data sensitivity

03.13.11 - Cryptographic Key Management:

- Encryption keys are created, stored, distributed, and signed securely
- Key management procedures are documented
- Cryptographic modules are validated per FIPS standards

What "Fully Implemented" Means



The Showstopper Requirements

Encryption In Transit (Data Crossing Boundaries):

- **All CUI transmission encrypted** - CUI never transmitted in plaintext
- **TLS 1.2 minimum** - All encrypted traffic uses TLS 1.2 or higher (TLS 1.3 preferred)
- **Strong cipher suites** - AES-256-GCM, AES-256-CBC, or equivalent (no weak ciphers)
- **Certificate-based authentication** - Certificates used for server authentication
- **Certificate validation** - Clients verify server certificates to prevent MITM attacks
- **Protocol enforcement** - Systems configured to reject connections using deprecated protocols
- **No deprecated protocols** - TLS 1.0, TLS 1.1, SSL 2.0, SSL 3.0 explicitly disabled
- **Internal flow encryption** - Even internal data flows between components encrypted if carrying CUI
- **API encryption** - All API calls to/from system encrypted with TLS 1.2+
- **SSH for admin access** - SSH 2.0 with strong ciphers for privileged access (no Telnet)
- **Database traffic encryption** - Database connections encrypted with TLS or database-native encryption

Encryption At Rest (Data Stored):

- **Sensitive data identified** - CUI, PII, payment card data, authenticators all encrypted at rest
- **FIPS-approved ciphers** - AES-256 minimum for symmetric encryption
- **FIPS 140-2 validated modules** - Encryption modules are FIPS-validated
- **FIPS module certificates** - Certificate numbers from FIPS 140-2 validation provided
- **Multiple encryption levels acceptable** - File-level, database-level, table-level, column-level, or field-level encryption all acceptable
- **Key storage** - Encryption keys stored securely (not in same location as encrypted data)
- **Key rotation** - Documented procedures for periodic key rotation
- **Backup encryption** - Backups of encrypted data also encrypted
- **Database encryption** - Full database, table, column, or field-level encryption implemented
- **File system encryption** - File system encryption (BitLocker, LUKS, etc.) or application-level encryption for sensitive files
- **Third-party service encryption** - SaaS/IaaS services configured to encrypt data at rest

Boundary Protection:



The Showstopper Requirements

- **Firewalls deployed** - Perimeter firewalls at all external boundaries
- **Internal firewalls** - Internal network segmentation through firewalls or ACLs
- **DMZ deployment** - Public-facing components in demilitarized zone (DMZ) separate from internal systems
- **Network ACLs** - Access Control Lists restrict traffic to only needed flows
- **Least-privilege access** - Network configured to deny by default, allow only essential communication
- **Intrusion detection** - IDS/IPS deployed to detect and prevent unauthorized access
- **Egress filtering** - Outbound traffic filtered to prevent data exfiltration
- **Ingress filtering** - Inbound traffic filtered to only allow needed services
- **Network segmentation** - Network divided into zones/subnets with restricted inter-zone traffic
- **VPN protection** - Remote connections through VPN with encryption

Encryption Standards Reference

Approved Symmetric Encryption:

- AES-256-GCM (Galois/Counter Mode) - Preferred
- AES-256-CBC (Cipher Block Chaining) - Acceptable
- AES-128 - Minimum acceptable (AES-256 preferred)
- FIPS 140-2 validated implementation required

Approved Asymmetric Encryption:

- RSA 2048-bit minimum (4096-bit preferred)
- Elliptic Curve Cryptography (ECC) P-256 minimum
- FIPS 140-2 validated implementation required

FIPS 140-2 Validation Requirement:

- You must provide FIPS 140-2 module certificate numbers
- Encryption modules must be listed in NIST's validated crypto modules list
- Off-the-shelf validated modules (OpenSSL, BoringSSL with FIPS mode, NSS FIPS, etc.) are acceptable

Implementation Example: End-to-End Encryption

CUI Data Flow from User to Database:

1. **User to Web Portal:** TLS 1.2 with AES-256-GCM cipher, mutual certificate authentication
2. **Web Server to Application:** Internal encrypted API call using TLS 1.2



The Showstopper Requirements

3. **Application to Database:** Database connection using TLS 1.2 + database-native encryption
4. **Database at Rest:** Column-level encryption of CUI columns with AES-256-CBC, FIPS 140-2 validated HSM

Encryption Key Management:

- Keys generated and stored in Hardware Security Module (HSM)
- Keys never transmitted in plaintext
- Keys rotated annually
- Backup keys generated and stored separately
- Key derivation documented for audit

GSA Review Checklist for 03.13.01 / 03.13.08 / 03.13.11

- Is encryption documented for all CUI data flows?
- Is TLS 1.2+ used for all data transmission (not TLS 1.0/1.1)?
- Are encryption cipher suites identified and strong (AES-256)?
- Are deprecated encryption protocols explicitly confirmed absent?
- Is encryption used for both internal and external data flows carrying CUI?
- Is data at rest encryption documented for all sensitive data types?
- Are FIPS-approved encryption algorithms used?
- Are FIPS 140-2 validated encryption modules documented with certificate numbers?
- Are encryption key management procedures documented?
- Is key storage secure (not in same location as encrypted data)?
- Is key rotation procedure documented?
- Is boundary protection in place (firewalls, ACLs, network segmentation)?
- Is ingress/egress filtering documented?
- Are network security tools (IDS/IPS) deployed?
- Is DMZ segmentation shown in architecture?
- Are VPN connections encrypted with TLS 1.2+?

Common Implementation Gaps

- **Incomplete encryption coverage** - Some CUI flows encrypted, others not
- **Deprecated protocols in use** - TLS 1.0, TLS 1.1, or SSL still enabled
- **Weak cipher suites** - Using DES, RC4, or other weak ciphers
- **No FIPS validation** - Using unvalidated encryption modules



The Showstopper Requirements

- **Missing encryption key documentation** - No documented key management procedures
- **Unencrypted sensitive data at rest** - PII or authenticators stored in plaintext
- **No boundary protection** - Systems directly connected to untrusted networks without firewall
- **No network segmentation** - All systems in flat network without access controls
- **Incomplete firewall rules** - Firewall configured but allowing unnecessary traffic
- **No egress filtering** - Outbound traffic not restricted, allowing potential data exfiltration

Showstopper #5: System and Information Integrity (03.14.01)

Requirement Title

Identify, Patch, and Track System Flaws

What GSA Is Checking

Your organization must have a flaw remediation program that[1]:

1. **Identifies flaws** through automated and manual processes
2. **Evaluates flaw severity** using defined criteria
3. **Remediates flaws** according to security-based timelines
4. **Tracks remediation status** through completion
5. **Prevents deployment of flawed software** before patches available
6. **Detects unauthorized changes** to system components

What "Fully Implemented" Means

Flaw Identification and Remediation:

- **Patch management program** - Documented process for identifying, testing, and deploying patches
- **Vendor alert monitoring** - Process for receiving security bulletins from software vendors
- **Security bulletin review** - Security bulletins reviewed for applicability to your systems
- **Patch testing** - Patches tested in non-production environment before production deployment



The Showstopper Requirements

- **Patch deployment schedule** - Defined timelines for deploying security-relevant patches
- **Urgent patch procedures** - Expedited procedure for critical/zero-day patches
- **Patch documentation** - Records of what was patched, when, and on which systems
- **Automated patch tools** - Tools like WSUS, Spacewalk, or cloud provider tools used for patch management
- **Mobile device patching** - Procedure for patching mobile devices accessing system
- **Firmware updates** - Firmware for network devices, storage systems, etc. also patched
- **Dependency tracking** - Understanding patch dependencies and deployment order
- **Post-patch verification** - Testing after patches to confirm successful deployment and system functionality

Unauthorized Change Detection:

- **File integrity monitoring** - Tools detecting unauthorized changes to critical files
- **Configuration management** - Documented baseline configurations for all systems
- **Change management process** - Formal approval process for authorized changes
- **Automated change detection** - Tools monitoring for configuration changes
- **Alerting on unauthorized changes** - Alerts when unauthorized changes detected
- **Incident response for changes** - Procedure to respond to detected unauthorized changes
- **Hash-based file monitoring** - Cryptographic hashing to detect file modifications
- **Database audit logging** - Schema and data change logging in databases
- **Application configuration tracking** - Monitoring application configuration changes

Malware Detection:

- **Antivirus deployment** - AV software installed on all systems capable of running it
- **Real-time scanning** - Continuous monitoring, not just scheduled scans
- **Signature updates** - Antivirus signatures updated regularly (daily or more frequent)
- **Quarantine procedures** - Detected malware isolated/quarantined automatically
- **Incident response for malware** - Defined procedure to respond to detected malware
- **Email scanning** - Incoming email scanned for malicious attachments/links
- **Web traffic scanning** - Web content scanned for malware before user access
- **USB/removable media scanning** - Scanning of removable media for malware
- **Antimalware tools** - Not just antivirus; detection of rootkits, trojans, spyware



The Showstopper Requirements

End-of-Life Software Handling:

- **EOL inventory** - Complete list of any End-of-Life software in use
- **Justification for EOL use** - If any EOL software retained: documented business justification
- **Risk evaluation** - Risk assessment documented for retained EOL components
- **Replacement plan** - Timeline for replacing EOL software with supported version
- **Compensating controls** - If replacement delayed: compensating security controls documented
- **Vendor support verification** - Confirmed through vendor communications that software is EOL

Patch Management Timeline Requirements

Vulnerability Type	Typical Timeline
Critical/Urgent	Within 14 days (or per CISA BOD)
High Priority	Within 30 days
Medium Priority	Within 60 days
Low Priority	Within 90 days

Table 3: Security Patch Deployment Timelines

Implementation Example: Patch Management Program

Weekly Security Update Process:

1. **Monday:** Microsoft/vendor security updates released
2. **Tuesday:** Security team reviews bulletins for applicability
3. **Wednesday-Thursday:** Patches tested in development/staging environment
4. **Friday:** Patches approved through change control if test successful
5. **First Tuesday of following week:** Patches deployed to production systems
6. **Post-deployment:** Verification scans confirm successful patch installation

Critical Zero-Day Response:

1. Vulnerability disclosed/exploited
2. Emergency change control initiated (within hours)
3. Temporary workaround deployed immediately (disable service, firewall rule, etc.)
4. Patch prepared and tested overnight
5. Production deployment within 24-72 hours depending on CISA timeline



The Showstopper Requirements

GSA Review Checklist for 03.14.01

- Is patch management program documented?
- Are vendor security bulletins monitored and reviewed?
- Is patch testing process documented?
- Are patch deployment timelines defined (security patches within X days)?
- Is there evidence of regular patch deployment (patch records)?
- Are urgent/critical patch procedures documented?
- Is antivirus/antimalware deployed on all systems capable of running it?
- Is real-time antivirus scanning enabled?
- Are AV signatures updated regularly (daily or more frequent)?
- Is file integrity monitoring implemented for critical systems?
- Is configuration management process documented?
- Is change detection enabled and monitored?
- Are EOL software components absent, or is risk mitigation documented?
- Is there evidence of patch/flaw remediation (deployment records, scan results)?
- Is post-patch verification performed and documented?
- Are malware incidents responded to per documented procedures?

Common Implementation Gaps

- **No patch management plan** - Patches deployed ad hoc without formal process
- **Slow patching** - Security patches taking 90+ days to deploy
- **No patch testing** - Patches deployed directly to production without testing
- **Incomplete coverage** - Some systems patched, others not
- **No critical patch procedure** - Same timeline for zero-day as routine patches
- **No antivirus** - Systems running without antivirus protection
- **Outdated signatures** - AV signatures not updated regularly
- **No file integrity monitoring** - No detection of unauthorized file changes
- **No configuration management** - No baseline configurations documented
- **No change detection** - Configuration changes occur without alerting
- **EOL software without justification** - Outdated software in use without documented risk mitigation
- **No evidence** - Claims of patching/remediation without supporting records



The Showstopper Requirements

Showstopper #6: System and Services Acquisition (03.16.02)

Requirement Title

Manage Unsupported Components and Vendor Risk

What GSA Is Checking

Your organization must manage the risk of unsupported (End-of-Life) software and third-party vendors[1]:

1. **Track all system components** and their support status
2. **Identify unsupported/obsolete components** and their risks
3. **Replace unsupported components** or document risk mitigation
4. **Assess vendor security posture** for all third-party providers
5. **Monitor vendors** for compliance with security requirements
6. **Prohibit vendors** from specific banned countries/companies

What "Fully Implemented" Means

Unsupported Component Management:

- **Complete component inventory** - All hardware, software, services documented with vendor and support status
- **Vendor support verification** - Current support status confirmed through vendor documentation
- **EOL identification** - Components no longer supported by vendor explicitly identified
- **Risk evaluation** - Risk assessment for each EOL component documenting residual vulnerabilities
- **Remediation timelines** - Replacement timeline for EOL components (e.g., "Windows Server 2008 to be replaced by Q3 2026")
- **Compensating controls** - If replacement delayed: documented controls reducing EOL component risk
- **GSA awareness** - EOL components disclosed to GSA with risk acceptance documentation
- **No unsupported encryption** - Encryption protocols below TLS 1.2 or weak ciphers not in use
- **No unsupported OS** - Operating systems no longer receiving security updates either replaced or mitigated
- **No unsupported libraries** - Outdated libraries and dependencies either updated or risk-accepted



The Showstopper Requirements

Vendor Security Management:

- **Vendor assessment process** - Documented procedure for evaluating vendor security
- **Vendor inventory** - Complete list of all vendors supplying components or services
- **Security requirements in contracts** - Contracts include security requirements for vendors
- **Vendor audit rights** - Contracts include right to audit vendor security compliance
- **Incident reporting obligations** - Vendors required to report security incidents affecting your system
- **Data protection requirements** - Contracts specify how vendor must protect your data
- **Subcontractor management** - Vendors required to apply same security requirements to subcontractors
- **Vendor assessment results** - Documentation of vendor security posture evaluation
- **Risk acceptance for high-risk vendors** - If vendor poses risk: documented risk acceptance
- **Continuous monitoring** - Ongoing process to monitor vendor security posture
- **Security certification verification** - SOC 2, ISO 27001, FedRAMP, or other relevant certifications verified
- **Financial stability assessment** - Vendor financial viability evaluated to prevent sudden closure
- **Background checks** - Key vendor personnel subject to background checks where applicable

Prohibited Vendor Technology:

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

- Kaspersky Lab (and any subsidiary)
- Huawei (and any subsidiary)
- ZTE (and any subsidiary)
- Hikvision (and any subsidiary)
- Hytera (and any subsidiary)
- Dahua (and any subsidiary)

Your obligation: Explicitly confirm these vendors are NOT used anywhere in your system or third-party integrations.

Supply Chain Risk Management (SCRM) Plan



The Showstopper Requirements

A required attachment to your SSPP, the SCRM plan must address[1]:

- **Vendor identification** - All vendors supplying components or services listed
- **Vendor assessment** - Security posture assessment for each vendor
- **Risk evaluation** - Risks introduced by each third party documented
- **Risk mitigation** - Specific actions to address identified risks
- **Continuous monitoring** - How vendor security posture monitored ongoing
- **Contract requirements** - Security clauses required in all vendor contracts
- **Incident reporting** - Procedure for vendors to report security incidents
- **Supply chain flow diagram** - Visual representation of how components flow from vendors into your system
- **Subcontractor assessment** - How vendors' subcontractors are assessed and managed
- **Alternative vendors identified** - If primary vendor fails: alternative sources documented

Implementation Example: Vendor Management

SaaS Platform Vendor Assessment:

1. **Initial Assessment:**
 - Request Security Documentation (SOC 2 Type II report)
 - Verify FedRAMP authorization status
 - Review incident response procedures
 - Confirm incident notification timeline
2. **Contractual Requirements:**
 - Include security requirements clause
 - Specify notification timeline for security incidents (24-48 hours)
 - Include audit right to verify compliance
 - Define data protection requirements
 - Specify subcontractor security requirements
3. **Ongoing Monitoring:**
 - Quarterly review of vendor security updates
 - Annual reassessment of vendor security posture
 - Monitor vendor financial stability
 - Track any reported security incidents
 - Verify SOC 2/ISO 27001 renewal



The Showstopper Requirements

4. Risk Acceptance (if needed):

- If vendor non-compliant: document risk evaluation
- Obtain GSA CISO approval for risk acceptance
- Implement compensating controls if possible
- Establish remediation timeline

GSA Review Checklist for 03.16.02

- Is system component inventory complete with vendor and support status?
- Are unsupported/EOL components identified with risk evaluation?
- Is replacement timeline documented for EOL components?
- Are residual EOL component vulnerabilities mitigated or accepted?
- Is vendor assessment process documented?
- Is vendor security management plan (SCRM) included as SSPP attachment?
- Are all third-party service vendors listed in SCRM plan?
- Are vendor security requirements included in contracts?
- Is there evidence of vendor security assessment (SOC 2, ISO 27001, audit results)?
- Are vendor incident reporting obligations documented?
- Is prohibited vendor check completed (Kaspersky, Huawei, ZTE, Hikvision, Hytera, Dahua)?
- Is continuous vendor monitoring process documented?
- Are alternative vendors identified for critical components?
- Is there evidence of ongoing vendor management (assessment records, monitoring reports)?
- Are subcontractors assessed and managed per same requirements?

Common Implementation Gaps

- **Incomplete component inventory** - Missing some hardware, software, or services
- **Unknown support status** - Components in use but support status not verified
- **EOL software without mitigation** - Outdated software in use without documented risk mitigation
- **No vendor assessment** - Third-party vendors used without security evaluation
- **Weak vendor contracts** - Vendor agreements lack security requirements and audit rights
- **No SCRM plan** - No documented vendor management or supply chain risk assessment



The Showstopper Requirements

- **Prohibited vendors in use** - Kaspersky, Huawei, or other prohibited vendors present
- **No incident reporting** - Vendor contracts don't specify incident notification procedures
- **No continuous monitoring** - Vendors assessed once but not monitored ongoing
- **No alternative vendors** - If primary vendor fails: no contingency plan documented
- **Subcontractors not managed** - Vendors' subcontractors not assessed or managed

Integration: How the Showstoppers Work Together

These six Showstopper categories form an integrated security posture[1]:

Defense-in-Depth Model:

1. **Access Control (03.01.02/03.01.12)** - First line of defense: control who can access the system
2. **Identification & Auth (03.05.03)** - Verify that the person requesting access is really who they claim
3. **Boundary Protection (03.13.01/03.13.08/03.13.11)** - Protect the perimeter and encrypt data crossing it
4. **Risk Assessment (03.11.02)** - Identify vulnerabilities that could allow unauthorized access
5. **System Integrity (03.14.01)** - Keep systems patched and free of flaws that could enable attacks
6. **Vendor Management (03.16.02)** - Ensure third-party vendors don't introduce vulnerabilities

Example Attack Scenario Prevented:

- **Attacker goal:** Exfiltrate CUI from the system
- **Showstopper #1 (Access Control)** blocks unauthorized entry through jump host
- **Showstopper #2 (MFA)** blocks credential-based attack even if password compromised
- **Showstopper #3 (Vulnerability Scanning)** identifies vulnerable component that could enable lateral movement
- **Showstopper #4 (Encryption)** prevents exfiltration even if attacker gains access to network traffic
- **Showstopper #5 (Patching)** prevents exploitation of known vulnerabilities
- **Showstopper #6 (Vendor Management)** ensures third-party vendors aren't introducing vulnerabilities



The Showstopper Requirements

Key Takeaways

1. **All six categories are mandatory** - Full implementation required for authorization[1]
 2. **Each has specific technical requirements** - Generic "security" is not sufficient
 3. **Documentation matters** - GSA reviewers will scrutinize your SSPP narratives against these requirements
 4. **Integration is critical** - The Showstoppers work together as a defense-in-depth model
 5. **Common gaps are preventable** - Understanding what GSA looks for prevents rework
 6. **Zero tolerance for some failures** - CISA KEV, residual EOL vulnerabilities, or prohibited vendors are automatic Showstopper failures
 7. **Technical expertise required** - Implementing these correctly requires security architecture expertise
-

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>