POLSINELLI

# Publications

March 6, 2026 • Updates

## New GSA Guidance on Protecting CUI in Contractor Systems, Plus a Look Ahead at Pending FAR Changes

### Key Takeaways:

- GSA released detailed procedural guidance for protecting CUI in nonfederal systems, and a proposed FAR rule would further standardize CUI handling, documentation and incident reporting across federal contracts.
- Together, these developments signal a shift toward uniform federal expectations for protecting CUI, driven by government priorities to standardize documentation, incident reporting timelines and contractor accountability across all agencies.
- Contractors should proactively review their CUI management practices, assess readiness against GSA's phased implementation roadmap and begin aligning incident-response procedures with anticipated FAR changes.

For many contractors, Controlled Unclassified Information (CUI) has been a moving target, identified through markings and agency-specific practices, with cybersecurity and reporting expectations that can look different from one procurement to the next.

The newest CUI development is the U.S. General Services Administration's (GSA) step-by-step procedural guide, which lays out how CUI is expected to be protected when it resides in nonfederal systems. Separately, a Federal Acquisition Regulation (FAR) Council proposed rule from last year would add a government-wide CUI framework to the FAR (including a proposed standard form and new clauses) — a useful indicator of the "direction of travel" on incident reporting and documentation expectations.

Together, these developments signal a push by the government toward more uniform expectations, especially around documentation, assessment discipline and faster incident escalation in contractor environments.

### GSA's 2026 CUI Guide: A Practical Roadmap for Protecting CUI in Nonfederal Systems

GSA issued Revision 1 of its IT Security Procedural Guide, *Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations Process,* on Jan. 5. The guide is an implementation roadmap organized around five phases — Prepare,

### Related People

- James W. Kim
- Erin L. Felix
- Sarah S. Glover
- Cate Baskin

### Related Capabilities

- Government Contracts
- Privacy & Cybersecurity

Document, Assess, Authorize and Monitor — that contractors can use to benchmark CUI documentation, assessment readiness and ongoing monitoring.

GSA says this process applies when CUI is handled in a contractor (nonfederal) system, the contractor is not operating that system on the Government's behalf and no separate law, regulation or policy imposes more specific safeguarding requirements. The requirements apply only to the components that process, store or transmit CUI (or provide security protection for those components), and the process requires coordination with and approval by GSA's Office of the Chief Information Security Officer (OCISO). In other words, scope is limited to the CUI boundary, and the process is structured around defined deliverables and approval gates.

**Notably for contractors, the guide reads like an implementation checklist — not a high-level policy memo. GSA condenses the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) into five phases and pairs each phase with concrete approval gates and recurring deliverables:**

Phase 1 – Prepare:

The "Prepare" phase starts with identifying and verifying the information types stored/processed/transmitted and determining the appropriate authorization path. GSA also expects vendors to categorize the system using a Federal Information Processing Standard (FIPS) 199 approach and notes that only nonfederal systems with a confidentiality categorization of "Moderate" are in scope (as CUI is in scope). GSA also describes a "solution readiness" briefing to confirm the architecture/boundary, key security capabilities and potential "showstopper" gaps before assessment.

Phase 2 – Document:

The "Document" phase of the guide shifts from concept to paperwork. Here, GSA lays out structured documentation steps that include privacy-related approvals, architecture submissions and an initial and then complete system security package (including a system security and privacy plan (SSPP)). The guide also calls for a Supply Chain Risk Management (SCRM) plan as an attachment to the SSPP (either a vendor plan consistent with NIST SP 800-161 or a GSA template).

Phase 3 – Assess:

GSA contemplates an independent assessment performed by a Federal Risk and Authorization Management Program (FedRAMP)-accredited Third-Party Assessment Organization (3PAO) or another assessment organization approved by GSA OCISO. Assessors must develop and obtain approval of a Security Assessment Plan (SAP) that sets expectations and bounds the level of effort, and the SAP must be approved by specific vendor and GSA roles before testing begins; otherwise, the vendor risks retesting. The guide also ties assessment results to remediation tracking. The plan of action and milestones (POA&M) must capture vulnerabilities (with limited exceptions), and the SSPP is expected to be updated to reflect the "as-implemented" state after assessment and remediation planning.

Practically, this means the SAP approval gate matters, and starting assessment work without it can create rework.

Phase 4 – Authorize:

The guide treats "Authorize" as the formal decision point after GSA review of the

assessment items and remediation plans, and it is structured like a security approval process rather than an informal “best efforts” checklist. This is a true decision gate, not a documentation formality.

Phase 5 – Monitor:

GSA requires ongoing monitoring deliverables. For example, it calls for quarterly submissions including vulnerability scanning reports tied to NIST SP 800-171 and a shared-drive access review, and it specifies timing (quarterly deliverables due one month prior to the completion of each government fiscal year quarter). The guide also addresses how changes are handled during the monitoring phase, including categories of changes and when pre-notification is required. This is where programs can often slip — navigating recurring deliverables and change control.

The guide also includes a dedicated incident response section. It emphasizes that reporting real and suspected incidents helps GSA and affected customers protect data and resolve issues quickly, and it states that incidents (or suspected incidents) do not result in punitive actions against a vendor, though failure to report will result in escalation. It also requires vendors to maintain current contact information for GSA security and contracting stakeholders, and it indicates that GSA’s Incident Response Team will initiate an incident and conduct follow-on reporting to the U.S. Computer Emergency Readiness Team (US-CERT) and the GSA Office of Inspector General (OIG), with customer notifications coordinated as needed.

**Ultimately, the guide provides a concrete “what good looks like” model, including defined phases, specific required deliverables (such as SAP, SSPP and POA&M), independent assessment discipline, recurring monitoring and clearer incident escalation expectations.**

## The Proposed FAR Rule: A Common Definition of CUI, a Standard Form and Compressed Incident Reporting

On Jan. 15, 2025, the U.S. Department of Defense (DoD),[1] GSA and NASA issued a proposed rule (FAR Case 2017–016) that would amend the FAR to implement the National Archives and Records Administration (NARA) CUI Program in federal solicitations and contracts. The public comment period closed on March 17, 2025. However, the FAR Council continues to list FAR Case 2017–016 as an open/active case and is processing public comments as part of developing a final rule. If finalized, the rule would apply CUI program requirements in federal contracts more uniformly.

Proposal highlights for contractors include:

- **Standardized way to communicate CUI requirements.** The proposal describes a new standard form (referred to in the preamble as “SF XXX”) intended to identify CUI requirements for a procurement and point contractors to agency reporting instructions.
- **Compressed incident reporting concept.** The proposed framework contemplates reporting suspected or confirmed CUI incidents **within eight hours of discovery** to an agency-designated website or POC.
- **Preservation expectations.** The proposal also discusses preserving and protecting system images and related information for **at least 90 days** after reporting unless the government declines interest.
- **Flowdown notice.** The proposed clause framework contemplates subcontractor incident notice up the chain, including an **eight-hour** concept.

Together, these concepts are a useful stress test for current incident response playbooks, vendor coordination and subcontract reporting clauses.

## Conclusion

GSA's 2026 guide makes clear that CUI protection is increasingly being evaluated as a managed program — documented, assessed, authorized and continuously monitored — rather than a one-time compliance exercise. At the same time, the pending FAR proposal signals that agencies may push for more uniform contract terms, including short-fuse incident notice and upstream reporting expectations. Contractors that tighten CUI boundary definitions, documentation packages and escalation paths now will be better positioned if these concepts become standard contract requirements.

If you have questions about how these CUI developments may affect your company, please contact Polsinelli's Government Contracts team. We advise government contractors on CUI compliance, cybersecurity obligations, incident response planning and related flowdown and documentation issues, and we are available to assist with readiness assessments, policy and contract review and response planning.

[1] President Trump signed an Executive Order on Sept. 5, 2025, renaming the Department of Defense to the Department of War. As of the date of this alert, published regulations continue to reference the Department of Defense, and this alert similarly retains this naming convention for consistency.