WINSTON & STRAWN LLP

BLOG

# Beyond the CMMC: New Cybersecurity Assessments for Government Contractors

FEBRUARY 18, 2026

The General Services Administration (GSA) recently announced changes to procedural guidance that may affect contractor eligibility for GSA contracts. GSA issued the IT Security Procedural Guide: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations Process CIO-IT Security-21-112, which set out a cybersecurity framework for protecting CUI that is similar to the Cybersecurity Maturity Model Certification (CMMC) for DoD contracts. The guidance sets forth both substantive cybersecurity requirements and an assessment process for those cybersecurity requirements, but differs from the CMMC in several important respects.

First, regarding substantive cybersecurity requirements, the guidance incorporates controls from NIST Special Publications 800-171 rev. 3, 800-172 rev. 3, and 800-53 rev. 5. This incorporates far more controls than the CMMC program, which is currently limited to controls from NIST SP 800-171 rev. 2. Second, unlike the CMMC Program, the guidance does not rigidly prescribe security controls. For example, the guidance explicitly contemplates a risk-based process wherein a contractor may seek certain deviations from substantive cybersecurity requirements, which the GSA can decide to accept. Third, the controls from NIST SP 800-53 rev. 5 only apply when personally identifiable information is in scope.

Regarding cybersecurity, the guidance sets forth a five-phase assessment process. Like the CMMC assessment process, the GSA's assessment process is complex and contains highly specific assessment requirements, such as certain deliverables due at the end of each stage in the assessment process. The chart below outlines the GSA assessment process:

**Table 1:** GSA's Five-Phase Assessment Process

| Phase | Description |
|---|---|
| 1. Prepare | Establish system scope, confirm information types, determine authorization path, and assess overall readiness.<br>***Key Deliverables and Activities*** |

| | |
|---|---|
| | • FIPS-199 categorization<br>• Determine if 800-171 or FedRAMP path applies<br>• Kickoff meeting<br>• System architecture briefing and readiness review (security capabilities, MFA, boundary, vulnerability management) |
| 2. Document | Fully document system architecture, security/privacy requirements, and all SSPP content.<br>***Key Deliverables and Activities***<br>• Complete SSPP using GSA template<br>• Integrated inventory workbook<br>• PTA/PIA (as applicable)<br>• Architecture Review Checklist<br>• SCRM Plan<br>• Initial/complete SSPP approval by GSA |
| 3. Assess | Conduct independent third-party assessment of implemented controls and generate required assessment artifacts. The independent third-party assessor must be either a FedRAMP-accredited 3PAO, or an assessment organization approved by the GSA OCISO prior to selection.<br>***Key Deliverables and Activities***<br>• Security Assessment Plan (SAP)<br>• Independent testing using GSA Test Case Workbook<br>• Vulnerability, configuration, and web app scans<br>• Security Assessment Report (SAR)<br>• POA&M<br>• Vulnerability deviation request sheet (if needed) |
| 4. Authorize | GSA evaluates residual risk and determines whether the system may be used to process CUI.<br>***Key Deliverables and Activities***<br>• Assemble full Security Approval Package<br>• GSA review for consistency, completeness, and risk<br>• ISSO/ISSM certification<br>• CISO approval and issuance of Memorandum for Record (MFR) |

| | |
|---|---|
| 5. Monitor | Ongoing monitoring and submission of recurring deliverables to ensure continued protection of CUI.<br>***Key Deliverables and Activities***<br>• Quarterly vulnerability scan reports and POA&M updates<br>• Annual SSPP and PTA/PIA updates<br>• Annual penetration testing (recommended)<br>• Triennial independent SAR |

GSA's decision to expand its oversight over cybersecurity controls for its contractors is consistent with the federal government's increased scrutiny of cybersecurity in procurement. Announced four years ago in October 2021, the Civil Cyber-Frauds Initiative utilizes the False Claims Act to pursue cybersecurity-related fraud by government contractors and grant recipients, resulting in increased DOJ settlements on cybersecurity cases. Consequently, Cybersecurity False Claims Act cases have reached an all-time high.

To avoid these legal issues resulting from noncompliance, companies that either hold or sell on GSA contracts requiring access to CUI should begin reviewing their covered systems and assess how they will implement GSA's cybersecurity requirements. While the requirements overlap to some degree with CMMC, GSA's framework contains broader requirements than CMMC. Thus, even current defense contractors that have been planning for CMMC for years must evaluate the additional requirements imposed by the GSA's framework.

3 Min Read

## Authors

Elizabeth Leavy

Lawrence S. Sher

Lawrence "Larry" Block

## Related Topics

United States Department of Defense

General Services Administration

Cyber Security

False Claims Act (FCA)

## Related Capabilities

White Collar & Government Investigations

Government Contracts & Grants

# Related Professionals

Elizabeth Leavy

Lawrence S. Sher

Lawrence “Larry” Block

*This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.*