wiley

ALERT

# Updates to NIST Cybersecurity Guidance May Impact Government Contractors

November 24, 2025

November 2025 has been a busy month for cybersecurity rules affecting government contractors. The long-awaited Cybersecurity Maturity Model Certification (CMMC) Program went into effect on November 10. We are now seeing the first Department of Defense (DOD) solicitations that include the CMMC Program requirements for contractors that process, store, or transmit Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) in performance of a DOD contract to adopt substantive security requirements based on the CMMC Level determined for the given work.

**NIST Seeks Additional Comments on Enhanced Security Requirements for Protecting Controlled Unclassified Information**

At the same time, the National Institute of Standards and Technology (NIST) has issued for public comment the Final Public Draft of its Special Publication (SP) 800-172r3 (Revision 3), Enhanced Security Requirements for Protecting Controlled Unclassified Information (CUI). SP 800-172 provides recommended cybersecurity controls for CUI on a nonfederal information system when associated with a "high value asset" or "critical program." SP 800-172 requirements are selected and imposed by federal agencies on certain contractors—and notably, select controls from the current version of this publication issued in February 2021 are incorporated as the CMMC Level 3 controls. The SP 800-172 controls are intended for safeguarding information that may be the target of "Advanced Persistent Threats" (APTs), which are highly capable, resourceful, and patient cybersecurity threat actors generally associated with nation-states such as China, Russia, Iran, or North Korea. The SP 800-172 Revision 3 requirements supplement NIST's SP 800-171 Revision 3, which was

## Authors


Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Vaibhavi Patria
Associate
202.719.4667
vpatria@wiley.law


## Practice Areas

Cybersecurity
Government Contracts
Privacy, Cyber & Data Governance

updated in June 2024, and are intended to be read in concert with NIST 800-171 Revision 3.

Alongside the draft SP 800-172 Revision 3, NIST has also released for public comment the Initial Public Draft of the companion assessment publication, SP 800-172A. This publication provides assessment procedures for organizations to determine whether they are implementing the security controls outlined in SP 800-172. The draft SP 800-172A has been updated to reflect the new controls added in both the November 2024 and September 2025 drafts of SP 800-172.

NIST last week extended the comment period for these publications to January 16, 2026.

When NIST last released a public draft of SP 800-172 a year ago, we noted the draft included new material on acquisition and supply chain risk management. In this latest round, NIST has added an additional fourteen (14) new controls that address, among other things, access controls, network segmentation, asset management, and more supply chain security practices. Of particular interest to those following the implementation of a Software or Hardware Bill of Materials (SBOM/HBOM), NIST added a requirement to create/maintain a "centralized repository for the inventory of system components." (03.04.08E). These additions are consistent with shifts in other NIST guidance, such as the Cybersecurity Framework, to more fully address the software supply chain.

**SP 800-172 Revision 3 May Become Part of CMMC Requirements, But Not Yet**

Contractors seeking CMMC Level 3 status must implement 24 of the controls from the February 2021 version of SP 800-172, and then obtain a Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) certification assessment of those controls. DOD has previewed that it may adopt newer versions of the SP 800-171 and SP 800-172 publications for CMMC, and that the Department would engage in future rulemaking if and when it chooses to adopt the revisions of those publications. This means that when Revision 3 of SP 800-172 and SP 800-172A are finalized, those controls would not immediately be incorporated into the CMMC Program.

Nevertheless, contractors may wish to start planning now how they might implement the new proposed SP 800-172 controls. In addition, federal agencies may choose to start implementing portions of SP 800-172 controls into selected contracts, grants, or other agreements involving particularly sensitive data—another reason contractors may want to get ready for the revised SP 800-172 even before revisions are adopted for the CMMC Program.

***

Wiley's cross-disciplinary Government Contracts, National Security, and Privacy, Cyber & Data Governance teams have significant experience advising clients on all aspects of compliance with CMMC requirements and will continue to monitor these developments.