wiley

ALERT

Contractors Should Prepare as NIST Finalizes Enhanced Security Requirements for Protecting Controlled Unclassified Information

May 15, 2026

On May 13, 2026, the National Institute of Standards and Technology (NIST) finalized a revision to Special Publication (SP) 800-172r3 (Revision 3), *Enhanced Security Requirements for Protecting Controlled Unclassified Information (CUI)*, which provides a selection of recommended cybersecurity controls for protecting CUI resident on a nonfederal information system when associated with a "high value asset" or "critical program." The revised publication highlights the importance of contractors being able to identify CUI and having plans to implement SP 800-172r3 controls even before the revisions are adopted into the Department of War (DOW) Cybersecurity Maturity Model Certification (CMMC) Program.

The SP 800-172 controls are tailored to protect CUI and associated systems that may be the target of "Advanced Persistent Threats" (APTs), which are cybersecurity threat actors generally associated with nation-states such as China, Russia, Iran, or North Korea that NIST assesses have the "expertise and resources" to use cyber, physical and deception capabilities to achieve their objectives. SP 800-172 Revision 3 is intended to supplement controls featured in NIST's SP 800-171 Revision 3 and SP 800-53: *Security and Privacy Controls for Information Systems and Organizations*.

Alongside SP 800-172 Revision 3, NIST revised the companion assessment publication, SP 800-172Ar3: *Assessing Enhanced Security Requirements for Controlled Unclassified Information*, to reflect new controls added to SP 800-172r3. This publication provides assessment procedures for organizations to determine how effectively an organization is implementing the security controls outlined in SP

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Erin M. Joe
Special Counsel
202.719.3140
ejoe@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Cybersecurity
Government Contractors & Grantees
Government Contracts
National Security

800-172r3. These publications do not immediately apply to contractors; however, agencies have required contractors to meet certain SP 800-172 requirements through terms of contracts, grants, or other agreements. For example, DOW selected certain controls from an earlier version (Revision 2) of SP 800-172 for its CMMC Level 3 requirement.

The SP 800-172 Controls Are Comprehensive but Flexible

The SP 800-172 controls are organized into 17 "families" of controls that together implement a defense-in-depth strategy with three components: penetration-resistant architecture, damage-limiting operations, and cyber resiliency.

For each control, NIST then describes the control, provides a discussion, maps the control to one of the three components of the defense-in-depth strategy, explains which adversary effects the control seeks to mitigate, and includes references to other NIST guidance if applicable. Some controls have "organization-defined parameters" (ODPs), through which federal agencies and nonfederal organizations who choose to implement these controls customize the implementation by selecting specific values (such as a tool, mechanism, or time period). The ODP concept provides flexibility in implementing these security controls.

As we have noted in previous updates on this publication, much of the new material focuses on acquisition and supply chain risk management and security practices. NIST also added new material for access controls, network segmentation, asset management, and threat detection. In total, NIST added 80 new controls, withdrew 12 controls, and made significant changes to 12 others. These revisions remain consistent with shifts in other NIST guidance, such as the Cybersecurity Framework 2.0, to more fully address the software supply chain.

New SP 800-172r3 Controls Raise Implementation Considerations for Contractors

Contractors seeking CMMC Level 3 status must have attained Level 2 certification, and also must implement 24 of the controls from the February 2021 version of SP 800-172 (Revision 2) and then obtain a Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) certification assessment. SP 800-172r3 and 800-172Ar3 will not be incorporated immediately into the CMMC Program – instead, DOW has indicated that it intends to engage in further rulemaking to update CMMC security requirements in the future.

Nevertheless, now that the revised SP 800-172r3 controls have been finalized, federal agencies may choose to start implementing new controls into select contracts, grants, or other agreements involving particularly sensitive data related to high value assets or critical programs – another reason contractors may want to be familiar with and have a plan to implement SP 800-172r3 controls even before revisions are adopted for the CMMC Program. Because the SP 800-172r3 controls assume that an adversary has the capability to target cybersecurity and physical security measures, planning should be cross-sectional and integrate personnel responsible for cybersecurity, physical security, and business continuity and resilience activities.

Further, because the SP 800-172 controls are intended to protect CUI residing in a nonfederal system and organization, the revised publication underscores the importance of contractors having a capability and process to identify CUI. In our experience, while the government is responsible for identifying and marking CUI to its contractors, some agencies have been aggressive in their designations. In an effort to reduce potential risk of mishandling, contractors may seek clarification or revision from the agency regarding their data labeling. However, if the government agency is not willing to revise marking decisions, then the agencies will expect those responsible for the data to follow handling procedures that apply to the data as marked.

****

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 CUI handling and CMMC requirements. Please reach out to any of the authors with questions.