wiley

NEWSLETTER

Cybersecurity Updates: NIST Publishes SP 800-171 Revision 3. What Changed, and What Comes Next?

June 2024

In May 2024, the National Institute of Standards and Technology (NIST) published Special Publication 800-171 Rev 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, and the accompanying assessment guide, 800-171A Rev 3, *Assessing Security Requirements for Controlled Unclassified Information*. Although the U.S. Department of Defense (DOD) has clarified that Revision 2 will continue to be the compliance standard for contractors that are subject to DFARS 252.204-7012, *Safeguarding Covered Defense Information*, until DOD announces otherwise, contractors should continue to think about how to comply with Revision 3's requirements in the event they become new standards for compliance. NIST applied both substantive and stylistic changes in Revision 3, which are covered below.

Path to Revision 3 and Beyond

In July 2022, NIST announced that it would update the series of publications concerning protecting controlled unclassified information (CUI). As part of updating the 800-171 publication, NIST solicited several rounds of public feedback through a pre-draft call for comments, an initial public draft, and a final public draft; NIST also sought comments on an initial draft of the 171A revision.

Overall, several of the style and content changes were intended to more closely align 800-171 with the federal baseline and guidance from NIST's 800-53 publications, which provide security and privacy controls for federal information systems. NIST has explained that it intends to bring the series of CUI-related publications into closer

Authors

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

Cybersecurity
Government Contracts
Privacy, Cyber & Data Governance

alignment with 800-53; we expect to see NIST's updates to other publications, such as 800-172 (*Enhanced Security Requirements for Protecting Controlled Unclassified Information*), similarly move closer to 800-53 in both form and content.

Summary of Key Changes in 800-171 Revision 3

Some of the notable changes and updates to NIST 800-171 in Revision 3 include:

- Updated to more directly align security requirements with 800-53 Rev 5;
- Introduced organization-defined parameters (ODPs);
- Added new tailoring criteria and recategorized certain controls based on those tailoring criteria;
- Added detail to clarify certain controls;
- Consolidated certain controls into multi-part requirements; and
- Identified supplemental materials (some still in progress).

Updates to Security Requirements (including ODPs)

Alignment With 800-53: NIST updated the security requirements to more closely align with 800-53 Rev 5, both substantively and stylistically. Notably, NIST added three new security requirement families to Revision 3 to maintain consistency with the 800-53B moderate control baseline: Planning (PL); System and Services Acquisition (SA); and Supply Chain Risk Management (SR). Additionally, NIST created certain multi-part requirements that subsume what were previously separate controls. As an example, security requirement 03.01.01, Account Management, was updated to incorporate items that were previously located under different requirements within Revision 2. Overall, NIST incorporated more detail into the requirements to bring them from high-level to something more tangible, both to more closely align with 800-53 Rev 5 and to clarify requirements with an eye towards language that would make assessing compliance with the requirements more straightforward and less subjective.

ODPs: NIST finalized the set of ODPs, which are identified in a table in Appendix D. NIST settled on 49 ODPs after fluctuations in response to industry and federal agency comments during the updating process. In FAQ responses released with Revision 3, NIST explained that the ODPs are intended "to provide flexibility to federal agencies in tailoring controls to support specific organizational missions or business functions and to manage risk," and to "help simplify assessments by providing greater specificity to the requirements being assessed and reducing ambiguity and inconsistent interpretation by assessors."

Commenters also asked NIST to identify who was responsible for defining ODPs; NIST noted that when a federal agency has not defined parameters for an ODP, nonfederal organizations should assign ODP values to the requirement. This may be welcome news for contractors that prefer to take a risk-based approach to defining ODPs that suit their organization's needs.

Tailoring: NIST added two new tailoring criteria: Not Applicable (NA) and Other Related Control (ORC). NA tailoring was applied to the Program Management (PM) and Personally Identifiable Information (PII) Processing and Transparency families, which are not allocated to a specific 800-53 baseline (i.e., Low, Moderate, or High). ORC was added to identify requirements for which the protection capability provided by the control is also provided by another control in the same or different control family, to lessen redundancy in the requirements.

NIST also eliminated the tailoring criterion that identified controls for non-federal organizations (NFO), because feedback from industry indicated that those controls were not being implemented or assessed in nonfederal organizations. NIST adapted or reassigned several previous NFO controls into NCO (not directly related to protecting the confidentiality of CUI), FED (primarily federal responsibility), and CUI controls.

Supplemental Materials

Several commenters asked NIST to create supplemental materials to help guide users through the changes in Revision 3, including mappings between Revision 2 and Revision 3. NIST provided an updated CUI overlay and change analysis spreadsheet with the release of Revision 3 and noted that it expects to issue several other mappings by the first quarter of 2025. These additional materials will include: a crosswalk between 800-171r3 and 800-171r2, 800-53r5, and the Cybersecurity Framework 2.0; and a 800-171r3 and 800-171Ar3 quick-start guide for small and medium enterprises.

For 800-171A Rev 3, NIST mapped the requirements to 800-53A, including hyperlinks to the 800-53A assessment procedures, and mapped the new categories for Planning, Systems and Services Acquisition, and Supply Chain Risk Management. NIST also created a new appendix that lists the ODPs.

Key Takeaways

DOD has made it clear through Class Deviation 2024-O0013 that it is not yet requiring contractors to implement Revision 3. We expect that DOD will take time to align federal and nonfederal stakeholders on how and when DOD will transition its compliance requirements to 800-171 Rev 3. This should include further guidance on whether, for which contracts, and how DOD will set ODPs; whether the Cybersecurity Maturity Model Certification (CMMC) proposed rule will go forward based on Revision 2 or transition to Revision 3; and what guidance will be given to assessors when DOD makes the transition from Revision 2 to Revision 3. In the meantime, civilian agencies could decide to require compliance with Revision 3 in agency-specific contract clauses, and the FAR Council is moving forward with its rulemaking to standardize contractual cybersecurity requirements across all agencies, which could also include Revision 3.

For all of these reasons, contractors should be thinking ahead to determine what changes they must make to implement new or revised security requirements identified in Revision 3, particularly as the CUI publications may continue to move closer to 800-53 with each iteration.