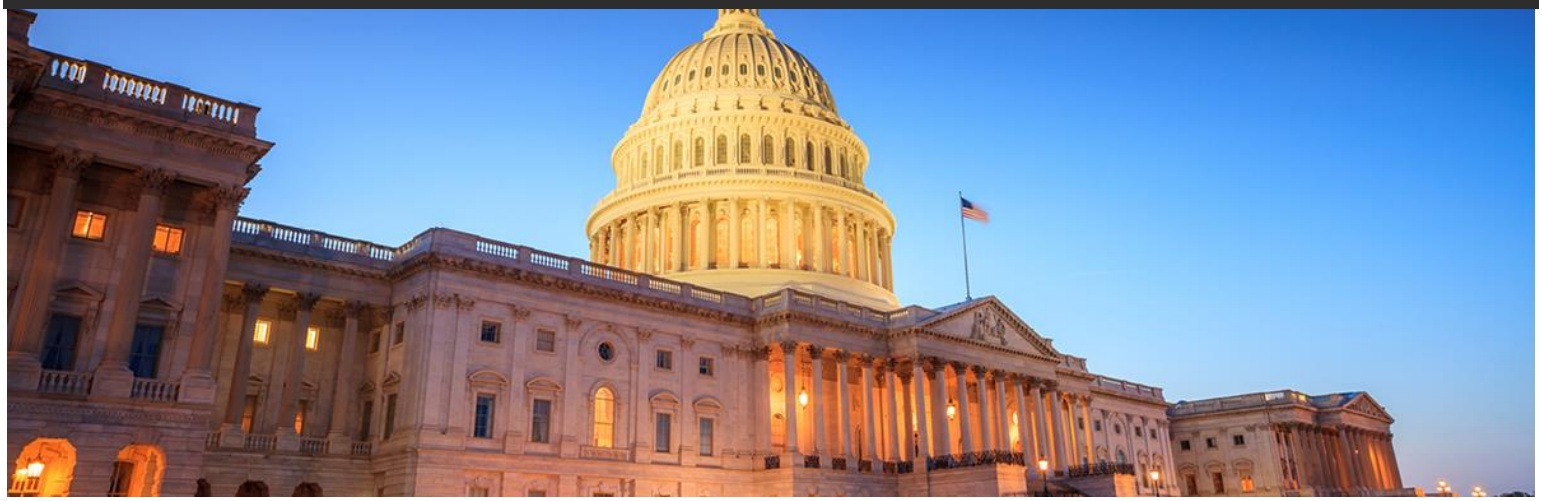
GT GreenbergTraurig

Alert | Government Contracts



June 2023

NIST Updates Guidelines for Protecting Sensitive Unclassified Info: Implications for Defense Contractors

Go-To Guide:

- Revision 3 to NIST SP 800-171 aligns controls with language in NIST SP 800-53 revision 5 and NIST SP 800-53B moderate.
- Changes may impact cybersecurity requirements imposed on Department of Defense (DoD) contractors.
- Contractors may be required to comply with Revision 3 once finalized.
- Contractors should monitor changes to regulations and ensure compliance with relevant updates.

On May 10, 2023, the National Institutes of Standards and Technology (NIST) released Revision 3 to its foundational publication, 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. The publication provides guidelines for protecting sensitive unclassified information in contractor systems, and these guidelines establish the baseline cybersecurity requirements for federal defense contractors. Systems that store controlled unclassified information (CUI) must meet the minimum requirements contained in NIST Special Publication (SP) 800-171.

NIST SP 800-171 rev. 2 currently provides the baseline cybersecurity controls imposed on defense contractors. Amid the in-progress Cybersecurity Maturity Model Certification (CMMC) rulemakings and existing self-assessment requirements, this GT Alert discusses the changes Revision 3 introduces and implications for contactor obligations and cybersecurity regulations.

According to NIST, Revision 3 is intended to align with updates to the security controls governing federal systems. Thus, many changes reflect updates to controls corresponding to the security requirements and families included in NIST SP 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020), and the NIST SP 800-53B moderate-control baseline. In particular, three new families have been added to Revision 3: Planning, System and Services Acquisition, and Supply Chain Risk Management.

Revision 3 retains approximately the same overall number of controls, with some requirements added and others withdrawn. Most of the withdrawn requirements are addressed within other controls. Revision 3 introduces updated tailoring criteria, increased specificity for security requirements, and organization-defined parameters for selected controls. The revision is also accompanied by a prototype CUI overlay providing a detailed analysis of the tailoring decisions at the control or requirement item level between SP 800-53 and SP 800-171. Compared to prior publication revisions, Revision 3 removes the distinction between basic and derived security requirements and includes more directives regarding implementation of the controls.

The revision was released in draft form, and comments are open until July 14, 2023. NIST specifically is interested in comments, feedback, and recommendations in the following areas: re-categorized controls (e.g., controls previously considered inapplicable), inclusion of organization-defined parameters, and the prototype CUI overlay. NIST has provided a "comment template" to facilitate the adjudication of comments. Prior to releasing the final version, NIST anticipates issuing Revision 3 in draft form at least one additional time. During a recent webinar, NIST also stated that it plans to release a draft version of NIST SP 800-171A to reflect the revised requirements in Revision 3 at the same time it releases the second draft of Revision 3.

Key Takeaways

Contractors may wonder what impact Revision 3 will have on current and upcoming cybersecurity compliance requirements. Currently, NIST SP 800-171 rev. 2 provides the framework for most cybersecurity controls imposed on the defense industrial base. Yet this new revision has been developed with the clear understanding that it will provide the basis for the future assessment of government contractors.

One of the main changes in the revised publication is an increase in the level of detail and specificity in the controls. NIST explains that this is intended to "remove ambiguity, improve the effectiveness of implementation, and clarify the scope of assessments." NIST recognizes that some organizations favored the broader, more abstract approach in prior versions of the publication, but notes that it often left requirements open to interpretation, making assessments difficult. The focus on developing controls in a manner that facilitates assessment is consistent with the use of the publication as the baseline for current and future cybersecurity requirements.

While the precise manner in which Revision 3 will be imposed on contractors is not yet known, Revision 3 will begin to be incorporated in contracts once it is finalized. The current regulations offer potentially conflicting obligations for defense contractors:

- **Defense Federal Acquisition Regulations Supplement (DFARS) 252.204-7012**: The -7012 clause requires compliance with the version of SP 800-171 "in effect at the time the solicitation is issued or as authorized by the Contracting Officer." Once Revision 3 is finalized the language of -7012 indicates that "covered contractor information system[s] shall be subject to the security requirements" in that version.
- **DFARS 252.204-7019 and -7020**: The NIST Self-Assessment provisions of the DFARS require contractors to conduct an assessment "in accordance with the NIST SP 800-171 DoD Assessment Methodology," which is provided on the DoD website. This methodology is based on Revision 2. Even after Revision 3 is finalized, it is unclear when the assessment methodology will be updated to correspond to Revision 3 and NIST SP 800-171A, rev. 1.

The current language of the cybersecurity requirements in the DFARS may result in a situation where contractors are required to comply with Revision 3 under -7012, but also are required to assess themselves in accordance with Revision 2. To mitigate or avoid these potentially conflicting requirements, DoD may issue a class deviation to avoid imposing Revision 3 on contractors before the assessment methodology has been developed. This would ensure that contractors are required to comply only with Revision 2 while the assessment methodology and associated requirements are updated to reflect Revision 3. It would also give contractors time to plan for implementation of Revision 3.

By the end of 2023, DoD intends to issue a Defense Industrial Base Cybersecurity Strategy that will identify the "pieces and parts" overlaying the NIST cybersecurity framework. This strategy may clarify the approach DoD intends to take to incorporate Revision 3 into DoD cybersecurity requirements. The issuance of this strategy will dovetail with the development of the CMMC program, which may not be implemented until fall 2024, according to the latest DoD pronouncements. CMMC 2.0 is based on Revision 2, which will likely be outdated by the time of the program's start. DoD may decide to revise its assessment methodologies to reflect Revision 3 and SP 800-171A, rev. 1 prior to implementing the CMMC program. While NIST's release of SP 800-171A, rev. 1 in conjunction with Revision 3 will likely facilitate the process of updating the CMMC and self-assessment methodologies, there is still likely to be some delay while those documents are developed following the finalization of the Revision 3 controls.

In the meantime, potentially impacted contractors should review the proposed controls and voice any concerns with the changes in Revision 3. The public comment period is open until July 14, 2023. Comments allow contractors to play a role in the requirements that ultimately will be imposed upon them. When submitting comments, contractors should consider using NIST's comment template, as well as ensuring that information is presented in a structured approach and feedback is supported with detailed rationales.

Authors

This GT Alert was prepared by:

- Eleanor M. Ross | +1 202.530.8565 | Eleanor.Ross@gtlaw.com
- Jeffery M. Chiow | +1 202.331.3149 | Jeff.Chiow@gtlaw.com

Francisco. Seoul.∞ Shanghai. Silicon Valley. Singapore.⁻ Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.