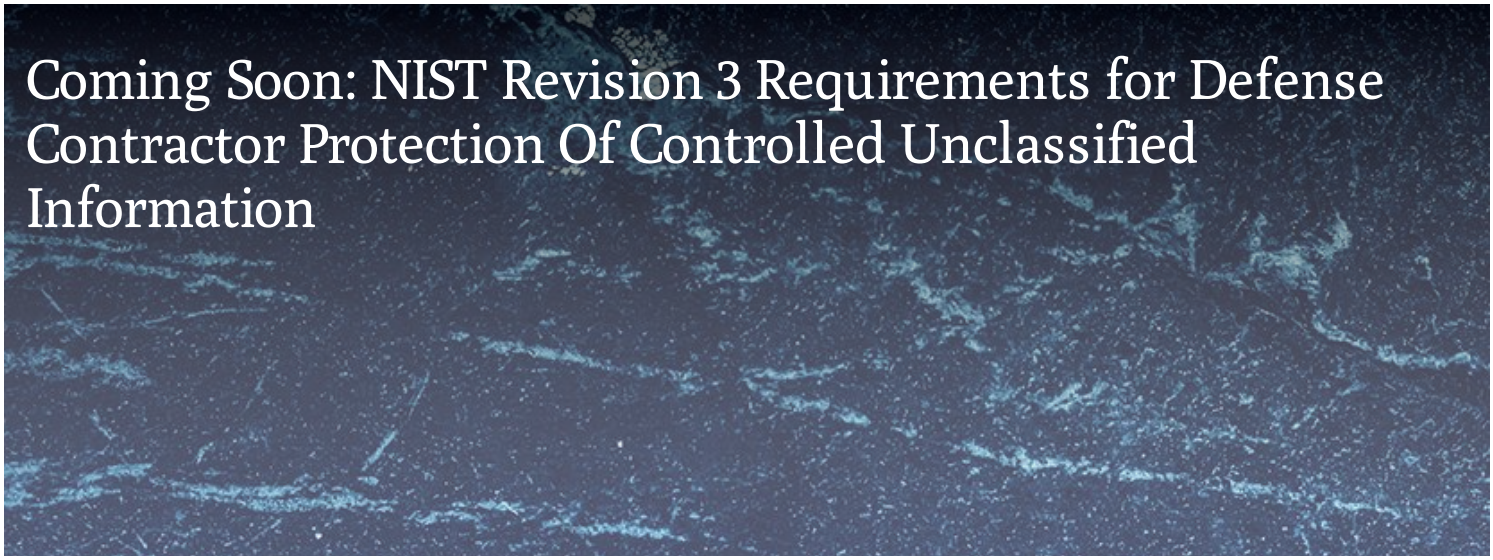
WINSTON & STRAWN LLP

BLOG

Coming Soon: NIST Revision 3 Requirements for Defense Contractor Protection Of Controlled Unclassified Information



OCTOBER 10, 2023

The National Institute of Standards and Technology (NIST) continues to update its guidance, through Special Publication 800-171 (NIST SP 800-171) on how defense contractors and subcontractors of federal agencies should protect Controlled Unclassified Information (CUI).[1] NIST SP 800-171 revision 3, which is expected to be published in early 2024, contains significant changes from the current version (revision 2).[2] Among many modifications, the initial public draft of revision 3, released on May 10, 2023, introduces new security controls, incorporates more detailed security requirements, and provides mechanisms for agencies to tailor their security requirements to their specific needs. These changes may require contractors currently handling CUI to review and revise their information security controls to remain in compliance with their contracts.

SCOPE OF NIST SP 800-171

NIST is a U.S. federal agency tasked with, among other things, developing standards for sensitive government information that is stored or handled by third parties.[3] NIST does not directly regulate, but rather establishes guidelines that federal agencies are able to adopt when establishing information security standards for CUI shared with and stored by third parties.

NIST SP 800-171 provides agencies with recommended security requirements for protecting the confidentiality of CUI when: "(1) the CUI is resident in a nonfederal system and organization; (2) the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and (3) there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry."[4] Accordingly, NIST SP 800-171 provides data security controls and guidelines on how contractors and subcontractors should manage and protect CUI. Where it is applied, NIST SP 800-171 requires contractors to implement 110 security controls to protect their information systems.[5]

NIST SP 800-171 must be applied in conjunction with NIST 800-53, which provides a larger "catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks."[6] These NIST

800-53 controls are mandatory for federal information systems, which are information systems used or operated by, or on behalf of, a federal agency.[7]

CHANGES TO NIST SP 800-171 IN REVISION 3

In the initial public draft of revision 3, NIST proposes various changes to security controls, families, and requirements from the predecessor revision 2. Revision 3 introduces organization-defined parameters (ODPs), which provide organizations with flexibility to change the requirements for certain security controls in order to tailor the security requirements to the agency's need. For example, requirement 3.1.8 expects contractors to limit the number of unsuccessful login attempts a user can make before they are locked out of the system. The exact number of attempts a user can make and the time frame in which a user is allowed to make them are both ODPs. Under revision 3, an agency would have the option to specify those numbers, provide guidance on how the contractor should select those numbers, or allow the contractor to choose the numbers on their own.[8]

The new revision also describes the required security controls with greater specificity. While revision 2 stated certain requirements at a high level, revision 3's more detailed descriptions mean that controls that were once open to subjective interpretation are now more tightly regulated. For example, revision 2, requirement 3.1.12 states that contractors must "[m]onitor and control remote access sessions."[9] In revision 3, the same requirement mandates five specific actions that a contractor must take to achieve the same goal of monitoring and controlling remote access sessions.[10]

Revision 3 also updates some of the tailoring criteria assignments—for example, to eliminate controls or parts of controls that are not directly related to protecting the confidentiality of CUI, or that are expected to be implemented by contractors without specification or direction by the government. Finally, with revision 3, NIST has provided a draft CUI overlay spreadsheet that describes how each control and control item is specifically tailored to protect CUI.

APPLICATION OF NIST SP 800-171

The most direct application of NIST SP 800-171 to contractors today is through the Defense Federal Acquisition Regulation Supplement (DFARS). For example, DFARS 252.204-7012 (7012 Clause) requires contractors subject to the clause to implement the security controls contained in NIST SP 800-171 if they handle CUI, and comply with other requirements such as the reporting of cybersecurity incidents. Importantly, the 7012 clause requires contractors to comply with the version of NIST SP 800-171 "in effect at the time the solicitation is issued or as authorized by the Contracting Officer."[11] To date, the Federal Acquisition Regulatory Council has not included a corollary version in the Federal Acquisition Regulations for non-defense contracts; however manufacturers, suppliers, and subcontractors should verify that the requirement to comply with NIST SP-800-171 is not included as a flow-down clause in their subcontract agreements with prime contractors.

Once finalized, defense contractors can expect to see the new requirements in forthcoming solicitations and contracts and may also see amendments to existing contracts to incorporate the new requirements. Public comments on the draft of revision 3 were due by July, 14 2023, and NIST anticipates publishing the final version in early 2024.

Relatedly, defense contractors will need to comply with the additional requirements in the forthcoming DOD Cybersecurity Maturity Model Certification 2.0 Model (CMMC 2.0). CMMC 2.0 is an updated cybersecurity assessment framework designed to evaluate the security of information systems of defense contractors, and will, among other requirements, require the implementation of the 110 security controls of NIST SP 800-171 in order to achieve at least a level 2 (out of three) rating under CMMC 2.0.[12]

COMPLIANCE RECOMMENDATIONS

While we await the final version, defense contractors should use this time to evaluate the initial public draft of NIST SP 800-171 revision 3 to identify gaps in their information systems and security controls to comply with the forthcoming requirements, including considering the following steps:

- Continue with ongoing efforts to comply with NIST SP 800-171 revision 2.

- Review changes set forth in NIST SP 800-171 revision 3 and the impact on individual contract(s).
- Evaluate necessary updates to security procedures to address and meet the requirements of NIST SP 800-171 revision 3.
- Contractors currently engaged in contracts subject to NIST SP 800-171 should monitor the release of revision 3 since new solicitations and modifications on existing contracts may require shorter-than-expected compliance with the requirements of revision 3.
- Where revision 3 is included in a new solicitation or proposed as a modification to an existing contract, consider raising with the Contracting Officer the timeline for compliance with revision 3, in order to seek adequate time for compliance.

Please contact the authors or your Winston & Strawn relationship attorney if you have any questions or need further information.

---

[1] NIST SP 800-171 Rev. 2, App. B at 72; *see also* NIST SP 800-171 Rev. 3 (Initial Public Draft), App. B at 72. CUI is defined as "[i]nformation that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended."

[2] Additional draft releases are possible. *See* https://www.nist.gov/news-events/news/2023/05/nist-revises-sp-800-171-guidelines-protecting-sensitive-information.

[3] NIST SP 800-171 Rev. 3 (Initial Public Draft).

[4] NIST SP 800-171 Rev. 2 at 2; *see also* NIST SP 800-171 Rev. 3 (Initial Public Draft) at 1-2.

[5] *See, e.g.*, NIST SP 800-171 Rev. 2 Security Requirement Spreadsheet, *available at* https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final.

[6] *See* NIST SP 800-53 Rev. 5 at ii, *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[7] *Id.* at 2.

[8] NIST SP 800-171 Rev. 3 (Initial Public Draft): Frequently Asked Questions, https://csrc.nist.gov/csrc/media/Publications/sp/800-171/rev-3/draft/documents/sp800-171r3-ipd-faq.pdf, May 10, 2023. ("Federal agencies can elect to specify ODPs, provide guidance on selecting ODPs for nonfederal agencies, or allow nonfederal agencies to self-select ODP values.").

[9] NIST SP 800-171 Rev. 2, 3.1.11.

[10] NIST SP 800-171 Rev. 3 (Initial Public Draft), 3.1.11. In order to comply, contractors must: "(a) [e]stablish, authorize, and document usage restrictions, configurations, and connections allowed for each type of permitted remote access, (b) [m]onitor and control remote access methods, (c) [r]oute remote access to the system through managed access control points, (d) [a]uthorize remote execution of privileged commands and remote access to security-relevant information, (e) [i]mplement cryptographic mechanisms to protect the confidentiality of remote access sessions."

[11] DFARS 252.204-7012(b)(2)(i).

[12] *See, e.g.*, https://www.federalregister.gov/documents/2021/11/17/2021-24880/cybersecurity-maturity-model-certification-cmmc-20-updates-and-way-forward.

7 Min Read

Authors

Lawrence "Larry" Block

Lawrence S. Sher

Elizabeth Leavy

William T. Kirkwood

Michael Hill

Related Topics

NIST | CUI | Defense Federal Acquisition Regulation Supplement | United States Department of Defense

Related Capabilities

Government Contracts & Grants

Related Professionals

Lawrence “Larry” Block

Lawrence S. Sher

Elizabeth Leavy

William T. Kirkwood

Michael Hill

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.