WILMERHALE

Compliance Deadline Reached for DoD Contractor Security Controls Requirements

JANUARY 4, 2018

Under the Department of Defense (DoD) final Defense Federal Acquisition Regulation Supplement (DFARS) rule on *Network Penetration Reporting and Contracting for Cloud Services*,[1] DoD contractors maintaining, processing, or otherwise possessing "covered defense information" (CDI) on their own systems must now be compliant with the technical, physical, and administrative security controls outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*,[2] as the "grace period" for compliance ended on December 31, 2017.[3] The rule's flow-down mandate requires that the applicable contract terms (and therefore the NIST SP 800-171 implementation requirement and deadline) be flowed down to all subcontractors whose performance will "involve" CDI or who are providing "operationally critical support."[4]

For more information on the final rule, see our summary and analysis of the final rule, available here, as well as our summary and analysis of the prior, interim version of the rule, available here. Our summary and analysis of the parallel Federal Acquisition Regulations (FAR) rule, which requires all federal government contractors (regardless of federal contracting agency) to abide by a subset of the NIST SP 800-171 controls if they have federal contract information, is available here.

Compliance Options

DoD contractors and subcontractors subject to the rule[5] have three options to ensure compliance with the rule's security standards:

1. Full Implementation. Contractors can comply with the rule's security requirements by fully implementing all security controls outlined in NIST SP 800-171 and documenting how those controls are met (or are otherwise inapplicable) in a System Security Plan (SSP).[6]

Ultimately, contractors are responsible for making their own determinations as to whether they are in compliance with the listed controls. DoD has stated that it will not certify contractor compliance with NIST SP 800-171 security controls, nor does it require, authorize, or recognize any third-party assessments or certifications.[7] However, NIST released two documents in November 2017 that

may be helpful to contractors trying to determine their implementation status:

- A "Self-Assessment Handbook," which "provides guidance on implementing NIST SP 800-171 in response to" the DFARS rule.[8] While the handbook was issued as part of NIST's Manufacturing Extension Partnership and is specifically intended to provide a "step-by-step guide [for] assessing a small manufacturer's information systems" and their compliance with NIST SP 800-171, this tool may be useful to all DoD contractors seeking to assess their own implementation of the NIST SP 800-171 controls.
- A draft NIST publication, NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information.[9]

2. Partial Implementation with "POAM." Contractors who have not yet been able to implement all NIST SP 800-171 security controls should endeavor to implement as many controls as possible, and document those controls in their SSP. Any controls that have not yet been fully implemented should be documented, along with the SSP, using Plan(s) of Action and Milestones, or POAM(s).

During a DoD-held "Industry Information Day" in June 2017, DoD officials indicated that contractors "complying" with NIST SP 800-171 partially through the use of POAMs would be considered in compliance with the broader DFARS rule's security requirements (and therefore would not, for example, be vulnerable to False Claims Act enforcement for failure to implement the control).[10] While DoD has not expressly confirmed this via formal written guidance, more recent DoD guidance has noted that SSPs can be used to document "[i]ndividual, isolated[,] or temporary deficiencies addressed by assessing risk and applying mitigations," and that, by December 31, 2017, "companies should have a system security plan in place, and associated plans of action to address any security requirements not yet implemented."[11] Of course, inaccuracies in certifications or material documents, including an SSP, could create a risk of a False Claims Act action.

That said, contracting officers can require or allow elements of the SSP (and any associated POAMs) to be included in a contractor's proposal, use the SSP as an evaluation factor, and/or incorporate the SSP by reference into the contract.[12] For example, contracting officers may require that proposals identify any security requirements not implemented at the time of award, or require in the solicitation that all NIST SP 800-171 requirements must be implemented by the time of award.[13] As such, contractors should (1) ensure that their SSPs are accurate and associated POAMs are achievable and followed and (2) be mindful of the possibility that noncompliance with any of the NIST SP 800-171 security controls, particularly the more significant controls, could harm their ability to win contracts.

3. Implement Alternative, Equally Effective Controls. Contractors can also comply with NIST SP 800-171 controls through "[a]lternative, but equally effective, security measures."[14] To be approved for such a deviation, a contractor must submit a written request to the contracting officer for consideration by the DoD Chief Information Officer (CIO).[15] However, NIST SP 800-171 is itself relatively flexible, and representatives from the DoD CIO's office have stated at public events that many, if not most, proposed "alternative" controls have actually been directly in compliance with the NIST SP 800-171 requirements, and, therefore, have not required approval for deviation.

Regardless of which option a contractor chooses, ongoing vigilance is critical to maintaining compliance. As new contracts are awarded, additional CDI is generated or obtained, security risks change, and best practices for protecting information and information systems evolve, contractors will need to continually assess their controls and update their SSPs. The DFARS rule specifically requires that contractors maintain "adequate security," which is, at a minimum, compliance with NIST SP 800-171. As such, even if a contractor complies with the NIST standard through one of the options described above, it still must ensure that its security practices and procedures provide "adequate security" for CDI.

DoD Resources

In addition to the materials described above, DoD has posted a number of resources regarding the rule under the "Cybersecurity" tab of the DoD Procurement Toolbox,[16] including the January 2017 version of the FAQs on the rule.[17] A revised FAQ document has been pending with DoD since at least June 2017, though the dedicated page on the Procurement Toolbox site continues to indicate that the update will be coming "soon."[18]

---

[1] 81 Fed. Reg. 72986 (Oct. 21, 2016), available here.

[2] The November 28, 2017, version of NIST SP 800-171 (Version 1.1) is available here.

[3] DFARS 252.204-7012(b)(2)(ii)(A). Prior to this date, for contracts awarded prior to October 1, 2017, contractors not in full compliance with the NIST SP 800-171 security standards were required to report to the DoD CIO, within 30 days of award, which NIST SP 800-171 requirements they had not implemented. *Id*. 252.204-7012(b)(2)(ii).

[4] *Id*. 252.204-7012(m)(1).

[5] The rule contains an exception for contracts solely for commercially available off-the-shelf (COTS) items of supply.

[6] *See* Department of Defense, *Implementing DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting: What Happens on December 31, 2017?* at 15, available here (hereinafter, What Happens on December 31, 2017?). While the requirement for an SSP was expressly added in Version 1.1 of NIST SP 800-171, contractors with contracts that are subject to the prior version of NIST SP 800-171 (Version 1.0) should still document their security controls using an SSP per a DoD note, available here.

[7] *See, e.g., What Happens on December 31, 2017?* at 13.

[8] Patricia Roth, *NIST Handbook 162, NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements* (Nov. 2017), available here.

[9] Ron Ross, Kelley Dempsey, and Victoria Pillitterri, Draft NIST Special Publication 800-171A, Assessing Security Requirements for Controlled Unclassified Information (Nov. 2017), available here.

[10] Slides from the Industry Information Day are available here. Video from the session is posted in the Cybersecurity Resources tab of DoD's "Procurement Toolbox" website, here.

[11] *What Happens on December 31, 2017?* at 15-16 (internal emphasis omitted).

[12] *Id*. at 16-17; *Frequently Asked Questions (FAQs) – Implementation of DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services* at A21 (Jan. 27, 2017), available here.

[13] *What Happens on December 31, 2017?* at 17.

[14] DFARS 252.204-7012(b)(2)(ii)(B).

[15] *Id*. When the CIO "has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective," a copy of the approval shall be sent to the contracting officer. *Id*. 252.204-7012(b)(2)(ii)(C). The preamble to the final rule states that the DoD CIO will typically respond to such requests within five business days. 81 Fed. Reg. 72990.

[16] Available here.

[17] Available here.

[18] *See* here.

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195

Stephen W. Preston

PARTNER

Chair, Defense, National Security and Government Contracts Practice

stephen.preston@wilmerhale.com

+1 202 663 6900