wiley

NEWSLETTER

As Deadline for Contractor Cybersecurity Compliance Looms, DOD Acknowledges Industry Gaps

November 2017

Government Contracts Issue Update

As the December 31, 2017 deadline approaches for contractors to implement NIST SP 800-171 cybersecurity requirements outlined in DFARS clause 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting), DOD recently issued guidance tacitly acknowledging that industry is not fully prepared to be compliant by the deadline, and outlining the process DOD will use to "transition" to full compliance. This update highlights important steps for contractors who are still working to become NIST SP 800-171 compliant.

The December 31, 2017 Deadline for NIST SP 800-171 Compliance

In August 2015, DOD issued an interim rule requiring defense contractors who have sensitive defense information residing on or transiting across their information systems to immediately implement the cybersecurity processes and protocols outlined in NIST SP 800-171. Following backlash from industry regarding the time and resources needed to comply with these requirements, in December 2015 DOD revised DFARS clause 252.204-7012 to include a two-year grace period for contractors to phase in NIST SP 800-171 compliant procedures.

Since then, the clause has required covered contractors to "implement NIST SP 800-171, ***as soon as practical***, but ***not later than December 31, 2017***." In the interim, contractors who did not yet fully comply with NIST SP 800-171 were required to "notify the DOD Chief

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Practice Areas

Government Contracts
Privacy, Cyber & Data Governance

Information Officer . . . within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award." Likewise, DFARS clause 252.204-7008 (Compliance with Safeguarding Covered Defense Information Controls) states that by submitting an offer, "the Offeror represents that it will implement the security requirements specified by [NIST SP 800-171] . . . ***not later than December 31, 2017***."

This scheme established a requirement for contractors to either comply with NIST SP 800-171, or devote best efforts to establishing compliance by the end of 2017. While the two-year grace period seemed generous at first, anecdotal evidence suggests that the majority of covered contractors will not meet the December deadline and need more time. In theory, this could create a situation in which many contractors would be in breach of DFARS clause 252.204-7012 after the ball drop ushers in New Year's Day.

System Security Plans and Plans of Actions and Milestones Can Smooth Out Compliance Gaps

For covered contractors who do not expect to comply fully with NIST SP 800-171 requirements by the deadline, a recent update provides measured relief. In December 2016, NIST issued SP 800-171 "Revision 1," which updated guidance on the use of system security plans (SSPs) and plans of action and milestones (POAMs) to document gaps in an organization's security posture and the actions the contractor plans to take to overcome them:

Nonfederal organizations should describe in a system security plan, how the specified security requirements are met or how organizations plan to meet the requirements. The plan describes the system boundary; the operational environment; how the security requirements are implemented; and the relationships with or connections to other systems. Nonfederal organizations should develop plans of action that ***describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented***.

NIST SP 800-171, Rev. 1 at 9. The update instructed contractors to use the SSP "to describe any enduring exceptions to the security requirements," while "***[i]ndividual, isolated, or temporary deficiencies should be managed through [POAMs].***"

At least in theory, a contractor can meet the contractual obligation to comply with NIST SP 800-171 by either fully implementing the procedures and protocols it requires, or by documenting potential gaps in the contractor's SSP and outlining the contractor's "get well" plan in the POAM.

DOD's Updated Guidance for Implementing the Security Requirements of NIST SP 800-171

In a September 19, 2017 Memorandum addressing "Implementation of DFARS Clause 252.204-7012," Shay Assad (Director, DPAP) issued guidance to DOD acquisition professionals that acknowledges—if not expressly states—that contractors may not have NIST SP 800-171 compliant systems by DOD's December 31, 2017 deadline. In a section on "Documenting a Contractor's Implementation or Planned Implementation of NIST 800-171," the Memorandum calls out the short-term flexibility that may be gained from SSPs and POAMs that identify and provide a plan for overcoming compliance gaps:

To document implementation of the NIST SP 800-171 security requirements by the December 31, 2017 implementation deadline, companies should have a system security plan in place, ***in addition to any association plans of action to describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems***.

The Memorandum identified different methods that contractors have for informing the Government of the contractor's implementation of NIST SP 800-171 requirements, including gaps outlined in the SSPs and POAMs. For contracts issued prior to October 1, 2017, contractors still have an affirmative obligation to identify gaps to the DOD CIO. In other cases, the Memorandum notes "the solicitation may require or allow elements of the system security plan, which demonstrates/documents implementation of NIST SP 800-171, to be included with the contractor's technical proposal, and may subsequently be incorporated (usually by reference) as part of the contract." Contractors should view such disclosures to the Government as a best practice if information systems are not fully compliant with NIST SP 800-171, in order to avoid allegations in hindsight that the contractor failed to meet contract requirements outlined in DFARS clause 252.204-712, or made a material misrepresentation of compliance under DFARS clause 252.204-7008.

But contractors should also be aware that NIST SP 800-171 compliance could quickly become a competitive discriminator, especially for programs that will require access to sensitive covered defense information. The Memorandum highlighted the potential role of SSPs and POAMs in the source selection process, and noted that "the requiring activity is not precluded from using a company's [SSPs and POAMs] to evaluate the overall risk introduced by the state of the contractor's internal information system/network." Requiring activities are likely to develop "safeguarding requirements for a given procurement and the level of risk they are willing to accept as industry transitions to full compliance of the NIST SP 800-171 security requirements," and make case-by-case determinations about how they plan to evaluate compliance risk in individual competitions. In some cases, an agency may determine that it requires *all* security requirements in NIST SP 800-171 to be met for an offeror to successfully compete. In others, the agency may "determine whether to accept the risk of storing sensitive government data on a contractor system that has not fully met the NIST SP 800-171 requirements," and opt to incorporate the successful offeror's SSP and POAM into the contract "to ensure the contractor is held accountable to meet the NIST SP 800-171 requirements in accordance with its own plans."

Wiley Rein remains active in this area and has advised clients on the scope of DFARS clause 252.204-7012, the implementation of NIST SP 800-171 requirements, and compliance with cyber incident reporting obligations. If you have questions about any of these issues, please contact Jon Burd (jburd@wiley.law or 202.719.7172) or Matt Gardner (mgardner@wiley.law or 202.719.4108).