wiley

ALERT

DOD Issues Draft Guidance Showing Evolving Approach to Contractor Cybersecurity Requirements

April 25, 2018

WHAT: The Department of Defense (DOD) issued draft guidance for procurements that will require compliance with DFARS Clause 252.204-7012, Safeguarding Covered Defense Information, and implementation of National Institute of Standards and Technology (NIST) SP 800-171. The draft guidance includes a matrix of NIST 800-171 requirements that contractors and DOD agencies should prioritize when implementing NIST 800-171, and several approaches for DOD agencies to evaluate NIST 800-171 implementation during the source selection process. As discussed below, contractors should take note of four key takeaways from this draft guidance, and heed shifting expectations ahead of increasing scrutiny from agencies that are being pressed to more aggressively manage cyber risk.

WHEN: DOD issued the draft guidance on April 24, 2018, and comments are due by May 31, 2018. The draft guidance is open under DARS-2018-0023.

WHAT DOES IT MEAN FOR INDUSTRY: The draft guidance confirms that DOD's interpretation of DFARS Clause 252.204-7012 requirements and the manner in which DOD will assess compliance continue to evolve. The key takeaways from the draft guidance include:

1. DOD clarifies its (softer) expectation of what NIST SP 800-171 implementation means. One of the most common questions we receive from clients about DFARS Clause 252.204-7012 involves what a contractor should do if it has not yet implemented NIST SP 800-171 requirements. The Federal Register posting provides further evidence that DOD has softened the standard for meeting the contractual

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Government Contracts

Patent and Data Rights Counseling and Disputes

Privacy, Cyber & Data Governance

obligation in DFARS Clause 252.204-7012 and what it means for a contractor to "implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017." As that deadline approached last year and industry *writ large* was not fully prepared to demonstrate or certify that all NIST 800-171 requirements were met, DOD walked back the implementation requirement and began to adopt an interpretation of the DFARS clause that would allow contractors to demonstrate contractual compliance either by implementing all of the NIST 800-171 requirements, or by establishing a System Security Plan (SSP) that outlined the contractor's current state of compliance and identified compliance gaps, ***and preparing a plan of actions and milestones (POAM) for completing the implementation in the future***. We wrote in November about implicit guidance the Director of Defense Procurement and Acquisition Policy, Shay Assad, issued to that effect, and several media outlets reported the Undersecretary of Defense for Acquisition, Technology and Logistics, Ellen Lord, testified before Congress at the end of December about a similar interpretation. Now, we have further confirmation of this interpretation that would allow a contractor to comply with its contractual obligations by demonstrating a plan for implementing NIST 800-171 requirements in the future:

To provide adequate security, the contractor must, at a minimum, implement NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." NIST SP-171 states that in order to demonstrate implementation or planned implementation of the security requirements in NIST SP 800-171, nonfederal organizations should describe in a System Security Plan how the specified security requirements are met, or how organizations plan to meet the requirements, and should develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented.

2. DOD prioritizes NIST 800-171 requirements. No, it is not terribly helpful. The draft guidance includes a guide for "Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented." It identifies every NIST 800-171 requirement and assigns a "DOD Value" from 1 (lowest priority) to 5 (highest priority). The DOD Value is intended "to assess the risk that a security requirement left unimplemented has on an information system, to assess the risk of a security requirement with an identified deficiency, and to address the priority for which an unimplemented requirement should be implemented." In theory, this priority scheme should help contractors identify DOD's prioritized requirements, and help acquisition officials weigh the relative risk associated with requirements an offeror or contractor has yet to implement. But, in practice, this priority scheme is not likely to be useful. The vast majority of requirements (91) are assigned the highest priority rating, versus only 19 receiving one of the lower priority ratings. This is largely reflective of the fact that NIST 800-171 already includes the most important security requirements culled from its predecessor, NIST 800-53. The lower-priority requirements tend to be the low-hanging fruit and comparatively easy to implement, making it clear that DOD prioritizes the implementation of the hardest (and most resource-intensive) requirements.

3. DOD is getting serious about assessing NIST 800-171 compliance during source selections. Shay Assad's memo (cited above) stated that DOD would begin to consider NIST 800-171 compliance as part of the Government's evaluation of proposals, and the draft guidance provides further guidance for "Assessing the State of a Contractor's Internal Information System in a Procurement Action." The guidance provides a series

of alternative approaches for DOD agencies to evaluate the extent of an offeror's NIST 800-171 compliance, from establishing minimum acceptability (or "Go/No Go") requirements to assessing implementation "as a separate technical evaluation factor." It anticipates offerors will submit copies of their SSPs and POAMs documenting their current implementation status and the path for future implementation. Moreover, the guidance contemplates that the Government will "[a]ssess/track implementation of NIST SP 800-171 security requirements after contract award," by in some cases requiring contractors to continue submitting revised/updated SSPs and POAMs after contract award. This means that contractors who rely on SSPs and POAMs to temporarily bridge the gap to full NIST 800-171 compliance will have to demonstrate progress toward that goal and will not be able to rely permanently on those plans.

4. DOD's approach is a harbinger of broader changes in Federal procurement regarding cybersecurity. DOD's guidance is only part of a broader narrative playing out across the Federal IT acquisition community involving cybersecurity. Federal officials have made clear their view that the entire contracting community—not just DOD contractors—needs to step up its game on cyber as part of the government's effort to increase federal agency accountability. They want companies working with the government to consider "mission risk" rather than mere compliance. The President made clear in Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, that agencies are under scrutiny, and that contractor supply chains and cybersecurity practices are of concern. The Executive Order would hold "heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises" and ordered a report on "cybersecurity risks facing the defense industrial base, including its supply chain." Consistent with that directive, the Department of Homeland Security (DHS) is taking a more muscular approach to federal agency cybersecurity, including actions to scrutinize supply chains, bar certain companies' products from agency use, and consolidate IT acquisition to better buy and manage technology. DHS, with GSA and other agencies, is identifying gaps between contractor practices and government expectations, and is modeling agency-specific requirements on the DFARS cyber clause. Policymakers also may draw on aggregate results of Defense Contract Management Agency (DCMA) audits to inform risk assessment and planning.

In light of DOD's request for comments on its proposed guidance and shifting national strategies on cyber that will impact DOD and other contractors, now is the time for industry to identify additional guidance or clarification that would be helpful, and how the Government can better collaborate with the private sector on cybersecurity in procurement.