Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

DFARS Cyber Rule Considerations For Contractors In 2018

By **Susan Booth Cassidy and Catlin Meade**
January 2, 2018, 2:06 PM EST

Susan Booth Cassidy

Catlin Meade

Since August 2015, defense contractors have been on notice that they were required to implement the security controls in National Institute of Standards and Technology Special Publication 800-171 no later than Dec. 31, 2017, on covered contractor information systems. Although the focus has been on meeting this deadline, contractors should add to their New Year's resolutions compliance with other areas of Defense Federal Acquisition Regulation Supplement 252.204-7012 (DFARS cyber rule) and confirm that their existing processes and procedures anticipate how the U.S. Department of Defense will measure compliance with the rule in the year to come. Summarized below are responses to some of the key questions that contractors should address come the new year.

What are the safeguarding requirements imposed by the DFARS cyber rule?

Defense contractors must provide “adequate security” for information systems that process, transmit, or store covered defense information (“CDI”). “Adequate security” means that defense contractors must “at a minimum” implement the security controls in NIST SP 800-171 in effect at the time a solicitation is issued or as authorized by the contracting officer. If a contractor wants to use alternate security controls or believes that a particular control does not apply, the contractor must obtain approval from the DOD chief information officer.

What does implementation of NIST SP 800-171 entail?

The DOD has clarified, both at public "industry days" and in internal guidance, that “implementation” of NIST SP 800-171 means having a system security plan (SSP) and a plan of action and milestones (POA&M) that accurately reflect the status of a contractor’s compliance with the NIST SP 800-171 security controls. This means that the SSP and POA&M should describe how a contractor intends to come into compliance with security control(s) that it has not yet fully implemented. Specifically, security requirement 3.12.4, which was added in Revision 1 to NIST SP 800-171, states that an SSP must “describe the boundary of [a contractor’s] information system; the operational environment for the system; how the security requirements are implemented; and the relationships with or connections to other systems.” If a contractor has an SSP and POA&M that accurately reflect the current status of its compliance with the NIST SP 800-171 security controls and its plan to achieve full compliance, that

contractor has "implemented" NIST SP 800-171 for the purposes of the DFARS cyber rule. Whether the contractor is providing "adequate security" would still need to be determined.

If a contractor has implemented NIST SP 800-171 and documented such implementation with an SSP and POA&M, is the contractor in full compliance with the DFARS cyber rule?

Not necessarily. The DFARS cyber rule requires defense contractors to provide "adequate security" for information systems that transmit, store, or process CDI. "Adequate security" is defined in the rule as "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information." In other words, the more sensitive the information, the greater the standard for protection.

Implementation of the NIST SP 800-171 security controls is the "minimum" required to achieve adequate security. Failure to meet the adequate security standard could put contractors at risk of breaching their contracts. Determining whether a contractor is providing adequate security requires an assessment by a contractor's information technology, contracts and legal team. Indeed, as new technologies emerge and the threats to information systems continue to evolve, contractors will need to continually monitor and assess the security of their information systems. In addition to internal monitoring and auditing, mature cybersecurity programs often incorporate third-party audits or assessments to help identify gaps and provide an objective view of system security. Compliance with all 110 security controls in NIST SP 800-171 is a necessary and important first step in that compliance assessment.

Do contractors need to have Revision 1 of NIST 800-171 incorporated into their contracts to take advantage of the DOD's "implementation" interpretation?

Because security control 3.12.4 (requiring an SSP) was added in Revision 1 to NIST SP 800-171 in December 2016, contractors have wondered whether they must modify all of their contracts to explicitly incorporate Revision 1 to take advantage of the "implementation" interpretation advanced by the DOD. In guidance issued by the director of the Defense Pricing/Defense Procurement and Acquisition Policy Office (DPAP) in September 2017, the DOD stated that "if Revision 1 of NIST SP 800-171 was not in effect at the time of the solicitation, the contractor should work with the contracting officer to modify the contract" to include Revision 1. From a practical standpoint, however, this could prove a challenge to both contractors and government procurement personnel given the large number of DOD contracts that were awarded prior to December 2016 and that are still in effect. The DOD appears to have recognized this conundrum because on Nov. 27, 2017, the DOD issued a "note" on the DPAP procurement toolbox website noting that "[e]ven without Revision 1 of the NIST SP 800-171 — the contractor may still document implementation of the security requirements with a system security plan." Although not a promulgated regulation, this note seems to indicate that the DOD will permit defense contractors to document implementation with the security controls in NIST SP 800-171 with an SSP and POA&M regardless of which version of 800-171 is incorporated into their contracts.

How can the DOD use an SSP and what impact could this have on defense contractors?

Revision 1 to NIST SP 800-171 provides that federal agencies may consider a contractor's SSP and POA&Ms as "critical inputs to an overall risk management decision to process, store, or transmit CUI [controlled unclassified information]" on a contractor's internal networks. DPAP has instructed procurement personnel that compliance with NIST SP 800-171 could be used as an evaluation criteria to permit the DOD to determine "whether it is an acceptable or unacceptable risk to process, store, or

transmit" CDI on a contractor's system. Similarly, the DOD could establish compliance with DFARS 252.204-7012 as a separate technical evaluation factor or identify specific security controls that must be implemented as a prerequisite for competing. Likewise, evaluation criteria could consider how the DFARS cyber rule has been incorporated into a company's incident response plan or how a prime contractor is ensuring compliance with the rule throughout its supply chain. Failure to comply with these requirements could impact a company's competitive standing for new DOD contracts.

Industry has long objected that SSPs are not appropriate for broad dissemination because they contain highly sensitive information about contractors' internal networks. It appears that the DOD has heard these concerns because DPAP's September 2017 guidance suggests that contracting officers incorporate the SSPs by reference as part of the contract rather than require them as submissions. Even so, the accuracy of the SSPs and POA&Ms and a contractor's follow-through on its POA&Ms are crucial because by incorporating the SSP and POA&Ms, the DOD could argue that compliance with those documents is a contractual obligation. Furthermore, there is no regulatory prohibition on a contracting officer seeking a copy of an SSP at a later date. This contractual obligation is further exacerbated by DFARS 252.204-7008, which provides that by submitting an offer, a contractor is representing that it has implemented the NIST SP 800-171 security controls, including the requirement for an SSP. Finally, at its June 2017 industry day, the DOD confirmed that the Defense Contract Management Agency will have a role in auditing contractor compliance with the DFARS cyber rule.

How could proposed draft NIST SP 800-171A impact defense contractors?

In November 2017, NIST released Draft Special Publication 800-171A, "Assessing Security Requirements for Controlled Unclassified Information." This publication is intended as guidance for organizations in developing assessment plans and conducting "efficient, effective, and cost-effective" assessments of the implementation of security controls required by NIST SP 800-171. NIST is seeking comments on the document through Jan. 15, 2018. NIST SP 800-171A is not currently imposed on contractors; however, assessments based on a final version of this document could be used in a variety of ways, such as the basis for identifying security-related weaknesses in a system, as an aid in source selection, or by the Defense Contract Management Agency when auditing contractor compliance with the DFARS cyber rule.

What are my obligations as to subcontractors?

Prime and higher tier contractors are required to flow down DFARS 252.204-7012 without change to all subcontractors when performance will involve operationally critical support or CDI. Thus, the DOD expects (1) contractors to flow down CDI to its subcontractors only if necessary for subcontract performance; and (2) confirm that those subcontractors that receive CDI are in compliance with the DFARS cyber rule. How that confirmation is done — via certification, audit, survey — involves an assessment as to the sophistication of each subcontractor and the sensitivity of the CDI being flowed to the supply chain. The costs/benefits of each approach is fact dependent and should involve collaboration by a contractor's contracts, legal, and information technology functions.

What are the potential consequences if the DOD determines that a contractor is not in compliance with the DFARS cyber rule?

There are a number significant adverse consequences facing contractors that are not in compliance with all the requirements of the DFARS cyber rule. These range from impacts on new awards, to adverse performance reviews, to possible False Claims Act actions. For example, if compliance with NIST 800-171

security controls is an evaluation factor in a DOD solicitation and a contractor's SSP and POA&Ms document numerous security controls still to be implemented, this could result in a downgrading of a proposal or even exclusion from the competitive range. Likewise, if a contractor suffers a cyber incident that impacts CDI that can be connected to noncompliance with the DFARS cyber rule, that contractor could face adverse performance reviews, termination for default, or even possible suspension/debarment action depending on the facts. Finally, to the extent there are inaccuracies in a contractor's 30-day gap assessment letters or in its SSP/POA&Ms, or it has not implemented other requirements of the DFARS cyber rule, a contractor may be vulnerable to possible False Claims Act actions under an implied certification theory. Although the government could face significant proof issues in such a claim, it is important that the contractor's documentation of its cyber compliance be accurate and updated on a regular basis.

Do I have a plan in place to react immediately in the event of a cyber incident?

It is not a question of if but rather when for most contractors worried about a cyber incident. Contractors' incident response plans should be modified to incorporate the unique requirements of the DFARS cyber rule. In the first hours of an incident, contractors will need to have existing processes and procedures that allow them to at least: (1) put their response investigation under privilege to allow a free exchange of information internally and to allow the law department to assess legal risks; (2) ascertain what data has been affected; (3) reach out to forensic and other IT experts (whose agreements have already been negotiated) for assistance with preservation obligations and forensic investigation; (4) implement a communications plan that considers possible disclosures to government customers, commercial customers, individuals, state regulators, the media, Defense Security Service, company employees, and law enforcement; and (5) incorporates a business continuity plan if certain systems or applications (i.e., email) have been disrupted. These are just some of the initial tasks and contractors need a multidisciplinary team in place to make decisions as the investigation, response, and remediation proceeds.

Conclusion

This rule applies to a large number of contractors and that number is expected to increase. In its third quarter scorecard for inclusion of the DFARS cyber rule, the DOD found that over 140,000 DOD contracts included DFARS 252.204-7012 in fiscal year 2016 and over 101,000 and counting as of the third quarter of FY 2017. NIST has stated that a Federal Acquisition Regulation rule that will impose the security controls of NIST SP 800-171 across the government is in process. It remains unclear if the other provisions of the DFARS cyber rule, such as cyber incident reporting, will be reflected in any new FAR rule. Nonetheless, contractors are likely to see increasing requirements in this area as both technologies and the cyberthreats to those technologies evolve.

Susan Booth Cassidy is a partner and Catlin Meade is an associate in the Washington, D.C., office of Covington & Burling LLP.