Bloomberg BNA

Federal Contracts Report™

Cybersecurity

Revised Cybersecurity Requirements Mean More Compliance Measures for Defense Contractors

BY KENNETH WECKSTEIN AND PAMELA REYNOLDS

On Dec. 30, 2015, the Defense Department (DOD) issued a second interim rule allowing defense contractors an extension until Dec. 31, 2017, to implement the National Institute of Standards and Technology (NIST) cybersecurity controls required by DOD's recently revised DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, and DFARS 252.204-7008, Compliance with Safeguarding and Covered Defense Information Controls. The revised DFARS contract clauses were issued effective immediately on Aug. 23, 2015. Many were concerned that, absent the extension, defense contractors would be unable to comply with the new requirements, that the rules lacked clarity, and that the cost of compliance, particularly for small businesses, would be very high. Some of the significant changes implemented Aug. 23, 2015, included:

1. *Expanded types of information to be safeguarded.* DFARS 252.204-7012 previously required safeguarding of only unclassified Controlled Technical Information (''CTI''), defined as technical information with a military or space application that is subject to controls. The new rules expanded the safeguarding requirements to include Covered Defense Information (''CDI''), which includes CTI plus three other categories of information. CDI includes unclassified information that: (1) is provided to the contractor by or on behalf of DOD in connection with the performance of the contract or; (2) is collected, developed, received transmitted, used or stored by or on behalf of the contractor in support of the performance of the contract; and (3) CTI or one of the following other types of information:

   - *Critical information (operations security).* Facts identified in the Operation Security process that are vitally needed by adversaries to guarantee unacceptable consequences for friendly mission accomplishment.
   - *Export control.* Unclassified information concerning certain items, commodities, technology, software or other information for which its export could have a negative effect on national security or nonproliferation objectives.
   - *Other information requiring protection.* Other information marked or identified as requiring safeguarding or other controls.

2. *Expanded rapid reporting requirement to include broader range of cyber incidents.* DFARS 252.204-7012 continues to require rapid reporting of cyber incidents, meaning the contractor must investigate and report an incident within 72 hours of discovery. The previous reporting obligation was limited to cyber incidents involving CTI. In comparison, the interim rule includes any cyber incident that affects ''an information system that is owned, or operated by or for, a contractor and that process, stores, or transmits [CDI]'', as well as cyber incidents that may affect the contractor's ability to provide ''operationally critical support.'' Opera-

Kenneth Weckstein is the head of Brown Rudnick's Government Contracts and Litigation Group. He represents clients on matters related to government contracts, complex civil litigation, and trade secrets law. Pamela Reynolds is a member of Brown Rudnick's Government Contracts & Litigation Group.

tionally critical support ''means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment or sustainment of the Armed Forces in a contingency operation.''

3. *Revised security controls tailored for contractor systems.* Previously, DFARS 252.204-7012 required contractors to implement specified security controls from NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. Under the revised rule, contractors now must implement all of the security controls required by NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. NIST SP 800-53 was drafted to apply to federal organizations, whereas NIST 800-171 is specifically tailored to contractors. According to DOD, NIST 800-171 should be easier for contractors to implement, while also increasing the protections for Government information.

Defense contractors should be seeing these new rules in solicitations and possibly in modifications to their existing contracts. For some contractors, the safeguarding and reporting requirements will be entirely new; others already may have implemented the previous version of DFARS 252.204-7012 (effective November 2013) or voluntarily adopted equivalent policies. Either way, the new rules could require significant changes to contractors' cybersecurity programs.

Contracting officers are directed to insert DFARS 252.204-7008 and 252.204-7012 in all solicitations and contracts, including commercial item contracts or small business set-asides, regardless of whether the rules would apply to the work contemplated. Therefore, contractors should consider the following initial steps:

1. Prior to submitting a proposal, confirm whether the solicitation contemplates CDI or operationally critical support and how CDI will be marked. If the solicitation is unclear, ask the agency to clarify those requirements.

2. Determine whether subcontractors will be involved with CDI or be expected to provide operationally critical support and ensure that DFARS 252.204-7012 is incorporated into those subcontracts without alteration.

3. Review the extent of compliance with NIST SP 800-171 and confirm that compliance can be achieved no later than Dec. 31, 2017. Some of the new requirements, such as the use of multifactor authentication, could involve significant time and money to implement. Failure to meet the deadline could constitute a breach of contract and result in damages and/or termination.

4. Ensure that the proposal identifies any proposed variance from NIST SP 800-171 per DFARS 252.204-7008(c)(2)(i). Otherwise, DOD may presume that the contractor will be in full compliance by Dec. 31, 2017.

5. Obtain a DOD-approved medium assurance certificate to rapidly report cyber incidents as required by DFARS 252.204-7012(c).

6. Per DFARS 252.204-7012(b)(1)(ii)(A), report within 30 days of award, all security requirements of NIST SP 800-171 that were not implemented at the time of award.

In light of recent high-profile data breaches, there is a legitimate need to better secure federal data, but the costs these rules will impose on contractors, both in time and money, will be high. Whether DOD has struck the right balance is yet to be seen. However, the recent extension is a step in the right direction. Comments on the second interim rule are due by Feb. 29, 2016.

  FCR ISSN 0014-9063