wiley

ALERT

DOD Issues Final DFARS Rule on Network Penetration and Cloud Computing

October 21, 2016

WHAT: The Department of Defense (DOD) has adopted a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to require covered contractors to implement certain cybersecurity safeguards and report data breaches within 72 hours, adopting NIST SP 800-171 as the baseline for covered information system security requirements, and standardizing security requirements for cloud-based services. The final rule implements two previously published interim rules, with only modest changes, that Wiley Rein previously covered in August 2015 (here) and December 2015 (here).

WHEN: Contractors are encouraged to implement the adequate safeguarding standards in NIST SP 800-171 as soon as practical, but no later than December 31, 2017, consistent with the December 2015 version of the interim rule. The other requirements for mandatory reporting and cloud services already apply.

WHAT DOES IT MEAN FOR INDUSTRY: The final rule made few material changes to the interim rules that have been in place for more than a year. Key changes included clarifying the definition of "covered defense information," formalizing the process when contractors seek to vary from the NIST SP 800-171 requirements, exempting contracts that are solely for the acquisition of commercially available off-the-shelf (COTS) items, and clarifying the security requirements that apply to cloud service providers.

OUR ANALYSIS:

The most significant aspects of the rule remain unchanged: the final DFARS clause 252.204-7012 requires contractors to provide "adequate security" (*i.e.*, the standards outlined in NIST SP 800-171) to covered

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

defense information on all covered information systems and to rapidly report any incidents involving those systems. While industry pushed back on the scope of the rule, noting in particular that the security measures can be particularly onerous for smaller businesses or barriers to entry for commercial item contractors, DOD determined that the "cost to the nation in lost intellectual property and lost technological advantage over potential adversaries is much greater than these initial/ongoing investments." DOD also left unchanged the rapid 72-hour reporting requirement, despite industry concerns that such rapid reporting poses myriad practical challenges.

While the heart of the rule and DFARS clause 252.204-7012 remain unchanged, the final rule does have at least four notable updates. First, the definition of "covered defense information" was clarified to include information that is either "controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry) that requires safeguarding or dissemination controls and is (1) marked or otherwise identified in the contract, task order, or delivery order, and provided to the contractor by or on behalf of DOD in connection with the performance of the contract; or (2) collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." The expanded definition of "covered defense information" is in line with the National Archives and Record Administration's (NARA) recent rule addressing "Controlled Unclassified Information," and includes all of the categories of information that are considered CUI. The final rule provides better clarity to the scope of the contractor's obligation by requiring the Government to either mark or expressly identify in the contract information furnished by the Government that will be subject to the safeguarding requirements (which is akin to a standard DOD first adopted when a previous version of DFARS Clause 25.204-7012 was issued in November 2013), but continues to make contractors responsible for determining whether information developed or received from third parties in the course of performance is "covered defense information." DOD considers this to be a "shared obligation" of the contractor to recognize and protect such information, despite industry concerns that it creates an undue burden.

Second, the final rule amended DFARS clauses 252.204-7008 and 252.204.7012 to clarify the procedure for contractors requesting limited exemptions from specific NIST 800-171 requirements, where specific requirements are "nonapplicable" or the contractor implements an "alternative, but equally effective" measure. The -7008 clause permits contractors to submit written requests to the Contracting Officer ***in their proposals, prior to award***, to vary compliance with NIST SP 800-171, and those requests will be adjudicated by a representative of the DOD CIO within a targeted five-day turnaround. The preamble also clarifies that while the rule does not require the Government to consider proposed deviations in the evaluation of proposals, there is nothing that precludes drafting the solicitation to include such an evaluation. The revised -7012 clause includes a similar process for submitting requests after award. For subcontractors, the revised rule clarifies that any requests to vary the implementation should be submitted directly to the Contracting Officer, with notice of the request furnished to the prime contractor (or next higher-tier subcontractor).

Third, DFARS clauses 252.204-7008 and 252.204-7012 were revised to include a limited exemption for use in solicitations and contracts that are solely for the acquisition of commercially available off-the-shelf (COTS) items. Despite this limited exemption, DOD determined that it is in the best interests of the Government to

apply these requirements for other commercial item acquisitions, as well as to acquisitions below the simplified acquisition threshold.

Finally, the final rule provided additional clarification on the security standards that apply to cloud-computing services and capabilities from Cloud Service Providers (CSP). Where contractors will store or transmit covered defense information on a cloud-based information system, the CSP should meet the Federal Risk and Authorization Management Program (FedRAMP) standard for "Moderate" compliance, as well as the final rule's cyber incident reporting requirements. The reporting obligation would extend to any incidents involving a shared infrastructure. These obligations may require significant modification to standard CSP terms and conditions, including any service level agreements (SLAs) that dictate the terms of a commercial vendor's cloud services, and DOD contractors who utilize cloud-based services for covered defense information should give careful attention to whether existing CSP vendor agreements meet these standards.