JONES DAY

SEPTEMBER 2015

COMMENTARY

New DOD Cybersecurity Rule Continues Onslaught of Federal Regulations for Government Contractors

The last few months have been busy ones for contractors as the U.S. government continues to rapidly issue new requirements in an attempt to catch up in the cybersecurity arena. While the government has not yet realized its goal of establishing a uniform baseline for protecting government data in the private sector, it continues to make progress. In the past few months, the government has updated guidelines establishing baseline requirements for contractors and has given direction to agencies regarding actions that should be taken in working with contractors. While these efforts continue to move toward harmonization, agencies, for the time being, are still approaching cybersecurity on an ad hoc basis, as demonstrated by the Department of Defense's ("DOD") recent interim rule. In this *Commentary*, we describe these rules and anticipated future developments.

Updated Standards and Direction to Agencies

In 2010, the U.S. government designated the National Archives and Records Administration ("NARA") as the executive agency responsible for developing a government-wide program for the protection of controlled unclassified information ("CUI"). In May 2015, NARA issued a proposed rule establishing requirements for federal agencies that handle CUI. The proposed rule also authorizes these agencies to impose requirements regarding safeguarding CUI on contractors working with them. NARA indicated that it is formulating a standard Federal Acquisition Regulation ("FAR") containing CUI requirements that should be used in all federal procurement contracts. NARA expects to publish this FAR provision in 2016.

As part of establishing required protection for CUI, NARA worked with the National Institute of Standards and Technology ("NIST") to create a set of security guidelines to be used by contractors working with CUI. NIST released these guidelines in June 2015 in NIST Special Publication 800-171 ("SP 800-171"). These guidelines build on standards previously established by NIST that regulate the protection of CUI on government information systems (found in NIST Special Publication 800-53 ("SP 800-53")). NIST and NARA developed the new guidelines with the understanding that certain standards in SP 800-53 would not be appropriate for privately owned and operated contactor networks. Importantly, the SP 800-171 guidelines are tailored for nonfederal information systems that contactors already have in place, with a goal of attempting to avoid requiring contractors to completely replace legacy information systems.

The SP 800-171 guidelines identify 14 security requirement families that draw from the requirements for federal systems found in SP 800-53 and the Federal Information Processing Standard Publication 200. These set the minimum level of information security a contractor should maintain in information systems processing, storing, or transmitting CUI. The SP 800-171 guidelines do not prescribe specific controls, tasks, or system requirements. Instead, the standards contain a set of requirements that are intended to overlap with contractors' existing security processes. Contractors can use a variety of solutions to satisfy these requirements. Further, the guidelines specify that contractors may implement alternative, but equally effective, security measures to satisfy a particular requirement. These alternative measures should be based on existing and recognized security standards. To assist contractors in implementing appropriate measures or identifying appropriate alternatives, Appendix D of the NIST Guidelines maps the CUI security requirements to similar already established security controls in ISO/IEC 27001/2 or NIST SP 800-53.

As mentioned above, the new NIST standards do not automatically apply to government contracts. Rather, they are designed to provide federal agencies with recommended requirements to include in agreements with nonfederal entities. NARA has directed agencies, however, to apply the new standards in future contracts, and it is anticipated that SP 800-171 will form much of the basis of the FAR clause NARA will soon propose. As such, contractors should review the requirements in SP 800-171 and determine whether they need to update their information security practices now, as opposed to waiting for the upcoming FAR clause.

The Office of Management and Budget ("OMB") has also issued draft guidance designed to provide direction to agencies in what they should require of their contractors in connection with CUI. Like the NARA proposed rule, OMB's draft guidance recommends that agencies require their contractors to meet the SP 800-171 guidelines. In addition to the baseline security requirements, however, the OMB draft guidance also requires agencies to include contractual mandates that contractors report "cyber incidents" (including both actual compromises and potential adverse effects) that affect CUI.

The OMB draft guidance also directs agencies to conduct their own assessments of contractors' information security to confirm that they are meeting required standards. To allow for this, the guidance recommends that agencies include in contracts provisions granting access to facilities, installations, operations, documentation, databases, IT systems, devices, and the personnel used in the performance of a contract. Agencies also are advised to seek certification and confirmation of sanitization of government and government-activity-related files and information at contract closeout.

Finally, the OMB directs the General Services Administration to develop a "business due diligence" service that will provide access to risk information that will include data collected from voluntary contractor reporting, public records, publicly available data, and commercial subscription data. At this point, it is unclear how this new service will drive requests for information from contractors to build the database, but it seems likely that agencies will use their supply chain risk management authority to impose requirements for information to be included in the due diligence system.

DOD Interim Rule

The DOD has been in the vanguard of imposing cybersecurity requirements on contractors, primarily through contract clause requirements in the DFARS. Citing "urgent and compelling reasons" to issue an Interim Rule that is effective immediately, the DOD has, among other things, expanded the scope of its existing DFARS cybersecurity provisions, strengthened its reporting requirements, and updated it to account for NIST's development of SP 800-171. As this clause is a mandatory flow-down clause, it carries ramifications for all prime contractors and subcontractors working in the defense industry.

In revising DFARS 252.204-7012, DOD expanded the scope of the information covered by the clause. The clause now protects all Covered Defense Information ("CDI"), which is defined to include information provided to the contractor by the government, or obtained by the contractor in performance of the contract, that is:

- Controlled technical information
- Critical information for operational security
- Export control information
- Any other information marked or otherwise identified in the contract as requiring safeguarding or dissemination restrictions.

The scope of these categories proves somewhat expansive. For example, export control CDI includes technology controlled by the International Traffic in Arms Regulations, the Export Administration Regulations, and sensitive nuclear technology information, as might be expected. But the clause also requires safeguarding of a contractor's export license applications as CDI. It also expands CDI beyond the concept of "information." It expressly applies to "items" and "commodities," apparently requiring contractors to report an adverse effect on export-controlled items as a cyber incident. Finally, the catch-all category seemingly expands CDI to cover any information properly marked by DOD, and it could require the reporting of incidents affecting privacy data and even proprietary business information. In addition to expanding the scope of coverage, DOD updated the DFARS clause to reference SP 800-171 as a baseline for information security standards a contractor must meet, as opposed to SP 800-53, which the prior version referenced.

The DOD incident reporting requirements have been redoubled as well. The deadline to report remains 72 hours from the time that the contractor discovers a cyber incident, as does the requirement to conduct a further review of the incident for evidence of compromised CDI across the contractor's network. Subcontractors are now required to report a cyber incident both to the government directly and "up the chain" to its higher-tier contractors, ultimately reaching the prime contractor. The provision also retains the obligation of contractors to maintain an image of all known affected information systems for 90 days. In addition to preserving the damage assessment information and providing it to the government, contractors will be required, upon request, to grant DOD access to "additional information and equipment that is necessary to conduct a forensic analysis." This provision could prove quite intrusive, and although the clause places limits on the dissemination of contractor information not created by or for DOD, the exceptions are quite broad and vaguely defined (e.g., "entities with missions that may be affected by such information") and may be difficult to enforce.

Cyber incident reports must be filed online at the DOD-DIB Cyber Incident Reporting & Cyber Threat Information Sharing Portal. Reporting an incident requires a medium assurance certificate that must be acquired from an External Certification Authority. Although most prime contractors likely have such a certificate already, some small business subcontractors may not. Contractors at all tiers should obtain a medium assurance certificate in advance as part of their cybersecurity plans.

Conclusion

Contractors working with the government should become familiar with the security requirements of the NIST Guidelines in SP 800-171 as the government is moving in the direction of using these criteria to establish baseline requirements for information security. Further, contractors must understand their monitoring and reporting requirements for cyber incidents, as these are also fast becoming staples in cybersecurity contract provisions. The recent actions by NARA, OMB, and DOD give clear indication as to the government's priorities in the cybersecurity arena, and those that do business with the government will gain the most competitive advantage by proactively offering solutions that are in line with these priorities.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Peter F. Garvin III
Washington
+1.202.879.5436
pgarvin@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Jay Johnson
Dallas
+1.214.969.3788
jjohnson@jonesday.com

J. Andrew Jackson
Washington
+1.202.879.5575
ajackson@jonesday.com

Jeff Rabkin
San Francisco
+1.415.875.5850
jrabkin@jonesday.com

Chad O. Dorr
Washington
+1.202.879.3795
cdorr@jonesday.com

Fernand A. Lavallee
Washington
+1.202.879.3486
flavallee@jonesday.com

Grant H. Willis
Washington
+1.202.879.3847
ghwillis@jonesday.com

Todd S. McClelland
Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

D. Grayson Yeargin
Washington
+1.202.879.3634
gyeargin@jonesday.com