The shifting sands of cybersecurity: DOD's interim rule further burdens contractors

August 26, 2015

The Department of Defense (DOD) earlier today issued an interim rule, effective immediately, that significantly increases existing cybersecurity requirements for DOD contractors. The requirements in the interim rule, **available here**, have broad applicability to DOD contractors at both the prime and subcontract levels, including commercial item and small business contractors. Contractors can expect these requirements to begin showing up in new DOD contracts immediately and should begin taking steps to ensure compliance.

The interim rule contains a number of new and revised DOD cybersecurity requirements. The key issues are summarized below.

Scope of the DOD requirements

The interim rule significantly expands the scope of the prior unclassified controlled technical information (UCTI) clause's safeguarding and reporting requirements. Whereas the prior UCTI clause applied only to unclassified controlled technical information, the new clause—now titled "Safeguarding Covered Defense Information and Cyber Incident Reporting"—applies more broadly to all "covered defense information."

"Covered defense information" includes controlled technical information as well as export controlled information, critical information related to operations security and *any other information* marked or otherwise identified in the contract that requires safeguarding under relevant law and policy, including private and proprietary business information. The interim rule further clarifies that the definition of "controlled technical information" does *not* depend, as it did under the prior UCTI definition, on whether the information "is to be marked" with applicable DOD distribution statements.

This expanded definition, coupled with the clause's broad flowdown requirement, means that the revised clause requirements likely will apply to virtually all DOD contractors at the prime and subcontract levels. The interim rule also revises Part 212 of the Defense Federal Acquisition Regulation Supplement (DFARS) to clarify that the rule's requirements are applicable to commercial item contracts and subcontracts.

Security controls

Additionally, internal contractor information systems that contain covered defense information are subject to new safeguarding requirements. The interim rule removes the clause's previously required security controls from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. DOD

Key contacts

Phillip R. Seckman
Partner, Denver
D +1 303 634 4338
phil.seckman@dentons.com

Erin B. Sheppard
Counsel, Washington, DC
D +1 202 496 7533
erin.sheppard@dentons.com

Michael J. McGuinn
Senior Managing Associate, Denver
D +1 303 634 4333
Michael.McGuinn@dentons.com

replaces those requirements with the controls from the recently-issued NIST SP 800-171, issued on June 18, 2015, and previously **discussed here**.

The National Archives and Records Administration (NARA) in May 2015 issued a proposed rule, **discussed here**, that would establish a government-wide policy related to the identification and safeguarding of controlled unclassified information. NARA stated in connection with that rule that it intended to promulgate a Federal Acquisition Regulation (FAR) clause that would apply the requirements of NIST SP 800-171 to contractors. The Office of Management and Budget (OMB) likewise recently proposed guidance seeking to require the use of these same NIST SP 800-171 controls on a government-wide basis for internal contractor information systems, **discussed here**. DOD's decision to use the same NIST standards proposed by OMB and NARA is a welcome step to achieve consistency in cybersecurity standards across the federal government.

DOD in the interim rule also creates a new clause, DFARS 252.204-7008, which states that a contractor prior to contract award can provide a written explanation to the government justifying deviations from the NIST SP 800-171 controls. The prior DFARS UCTI clause had a similar provision, although not required pre-award, allowing contractors to provide this written explanation related to the NIST 800-53 controls. Under the interim rule, if seeking a deviation, a contractor must explain: (i) how the company has in place alternative security controls that "compensate for the inability to satisfy a particular requirement" of the NIST SP 800-171 standards or (ii) that a particular control is inapplicable. The new clause likewise clarifies that the contractor may either comply with the NIST SP 800-171 requirements or provide for alternative but equally effective security measures, a determination which must be approved by DOD prior to contract award.

Reporting requirements

The interim rule also expands reporting obligations. The rule requires contractors that discover a cyber incident that affects a covered contractor information system or information contained therein to investigate and report that incident to DOD. As part of its implementation of Section 1632 of the 2015 National Defense Authorization Act, DOD also requires contractors to investigate and report a cyber incident that affects the contractor's ability to perform "operationally critical support" functions of a contract. Subcontractors are required to report cyber incidents to both the prime contractor and the government, with lower-tier subcontractors required to report cyber incidents up the chain of privity until the prime contractor is reached.

In addition, the rule modifies DFARS 252.204-7012 to permit DOD to release certain contractor information in a number of circumstances, including "to entities with missions that may be affected by such information" and "for national security purposes." This expands the permissible reasons for sharing included in the prior version of the clause, which had limited the government's use of contractor information only to "authorized persons for purposes and activities consistent with [the prior UCTI] clause." Because contractor information now may be disclosed outside the government, contractors should clearly mark information provided to DOD and carefully consider whether particular information should be disclosed in connection with a cyber incident.

The interim rule further establishes DFARS 252.204-7009, Limitation on the Use and Disclosure of Third-Party Contractor Reporting Cyber Incident Information.

This clause is required in contracts that involve contractor support for government activities related to safeguarding covered defense information and cyber incident reporting. It imposes nondisclosure obligations on contractors handling reporting information and provides that a contractor's breach of its nondisclosure obligations may be subject to criminal, civil, administrative and contractual actions brought by the government, or, importantly, by the impacted reporting party.

Cloud computing requirements

And if the foregoing was not enough, the interim rule also contains a number of new requirements relating to the acquisition of cloud computing services. The interim rule adds a new DFARS subpart, 239.76, which formalizes DOD guidance in this area and mandates that DOD may only award contracts for cloud computing services to contractors that have obtained a provisional authority to operate from the Defense Information Systems Agency (DISA). The new subpart requires the inclusion of specifically enumerated government protections in any DOD cloud services purchase order.

The interim rule also establishes two new contract clauses, DFARS 252.239-7009, Representation of the Use of Cloud Computing, and DFARS 252.239-7010, Cloud Computing Services, for use in any acquisition for information technology services. These clauses require contractors to: (i) implement administrative, technical and physical safeguards and controls outlined in DISA's Cloud Computing Security Requirements guide; (ii) maintain all government data in the United States unless authorized otherwise in writing; and (iii) restrict access to government data. DFARS 252.239-7010 also mandates that contractors report all cyber incidents related to the cloud services provided under the contract and imposes reporting and compliance obligations that parallel the access and investigation cooperation requirements included in the new UCTI clause.

Comments on the interim rule are due by October 26, 2015. Dentons lawyers will continue monitoring key developments in this area. Additionally, starting in the fall of 2015, Dentons lawyers will be presenting on behalf of the Public Contracting Institute a six-part series addressing the detailed compliance requirements and best practices relating to government contracts cybersecurity. More information about the series can be **found here** or by contacting the authors of this client alert.