THE
NATIONAL LAW REVIEW

DoD Addresses Cybersecurity Preparedness, Incident Reporting, and Cloud Computing Acquisitions with new DFARS interim rule

SheppardMullin

Article By
Alexander W. Major
Sheppard, Mullin, Richter & Hampton LLP
Government Contracts, Investigations & International Trade Law Blog

- Communications, Media & Internet
- Government Contracts, Maritime & Military Law

- All Federal

Wednesday, August 26, 2015

Announced and effective today, August 26, 2015, DoD has issued an interim rule that significantly expands existing DFARS provisions and clauses requiring contractors and subcontractors to report cyber incidents. The interim rule will apply "to all contractors with covered defense information transiting their information systems," an estimated 10,000 contractors. Additionally, in an effort to ensure acquisition uniformity across the Department, the interim rule implements DoD policies and procedures to be used when contracting for or utilizing cloud computing services. Due to "urgent and compelling reasons," the rule was issued without an opportunity for public comment.

The interim rule is an amalgamation of multiple statutes, manuals, and policies and it affects numerous DFARS clauses and provisions in implementing and consolidating requirements found in:

- Section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year 2013;

o Requiring cleared defense contractors to report penetrations of networks and information systems, and

o Allowing DoD personnel access to equipment and information to assess the impact

of reported penetrations

- Section 1632 of the NDAA for FY 2015;

o Requiring that a contractor designated as “operationally critical” must report each time a cyber incident occurs on that contractor’s network or information systems.

- A December 15, 2014, DoD Chief Information Officer (CIO) memorandum entitled “Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services”; and
- The January 13, 2015 DoD Cloud Computing Security Requirements Guide (SRG) Version 1, Release 1.

A brief rundown of the key elements of the interim rule is found below. However, for the cybersecurity issues, contractors should focus their attention on the newly refined cyber incident reporting procedures (now found at DFARS 204.7302(a)(1) and clause 252.204-7012(c)), including more exacting report requirements (although the reporting period remains at 72 hours); the reporting requirements of *all* subcontractors (now found at DFARS 204.7302(a)(2)); and the inclusion of new contractual clauses when “covered defense information” is at issue (now found at DFARS 204.7304).

Cloud service providers and contractors wishing to employ cloud resources should be aware that DOD will only accept “cloud computing services using commercial terms and conditions that are consistent with Federal law, and an agency’s needs.” Accordingly, a cloud provider – be it as a prime or as a subcontractor – must have received “provisional authorization by Defense Information Systems Agency, at the level appropriate to the requirement” (now found at DFARS 239.7602-1(b)). Furthermore, any “Government data” stored in the cloud and not resident on a DOD installation must reside on servers in the United Sates unless otherwise authorized (now found at DFARS 239.7602-2(a)). Contractors will also be obligated affirmatively to advise the government of their intent to use cloud services for their government data (now found at DFARS 252.239–7009).

Here’s an extremely brief rundown of what is new:

> **1. Definitions**: The definition of “Cyber incident” is unchanged but has been moved from DFARS 204.7301 to DFARS 202.1. Two new terms, “compromise” and “media,” are also included with the other definitions
>
> *a. cyber incident*: “actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.”
>
> *b. compromise*: “disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.”
>
> *c. media*: “as used in parts 204 and 239, means physical devices or writing

surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system."

2. DFARS subpart 204.73, Safeguarding Unclassified Technical Information, is to be expanded now to address protection of a broader collection of data and information described as "*covered defense information*" and adverse effects on a "contractor's ability to provide operationally critical support." The previous definition of "controlled technical information" remains, but the expanded provision includes many new definitions, the most pertinent being *Covered defense information*. That term is defined as unclassified information that is "(i) provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or (ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract" and that also falls into any of the following categories:

i. Controlled technical information.

ii. Critical information (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

iii. Export control. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations, and munitions list; license applications; and sensitive nuclear technology information.

iv. Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (e.g., privacy, proprietary business information).

"*Operationally critical support*" is also a newly defined term, referring to "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." Any "cyber incident" that affects such support is required now to be reported.

3. DFARS 252.204-7012 is to be renamed "*Safeguarding Covered Defense Information and Cyber Incident Reporting*." Reflecting the changes to DFARS subpart 204.73, the clause is expanded to address protection and reporting requirements related to "covered defense information" and will require contractors to report "cyber incidents" involving this new class of

information as well as any cyber incident that may affect the ability to provide "operationally critical support." Not surprisingly, the clause's previous reference and use of cherry-picked security standards found in NIST SP 800-53 has been replaced by reference to NIST SP 800-171, a recently released publication specifically tailored for use in protecting sensitive information residing in contractor information systems.

4. DFARS 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, is a **new provision** intended to make offerors aware of the requirements of clause 252.204-7012, while also allowing contractors an opportunity to explain to the DoD CIO: (i) how the contractor's alternative security measures can compensate for the inability to satisfy a particular requirement; or (ii) why a particular requirement is not applicable. The DoD CIO will then approve or disapprove the request to deviate with any approved deviation incorporated into the resulting contract.

5. DFARS 252.204-7009, Limitations on the Use and Disclosure of Third-Party Contractor Reported Cyber Incident Information, is a **new provision** added to protect information submitted to DoD in response to a cyber incident.

6. DFARS subpart 239.76, Cloud Computing, is a **new subpart** added to implement policy for the acquisition of cloud computing services.

7. DFARS 252.239-7009, Representation of Use of Cloud Computing, is a **new provision** added that requires the offeror to indicate whether it intends to use cloud computing services in performance of the contract.

8. DFARS 252.239-7010, Cloud Computing Services, is a **new provision** added to provide standard contract language for the acquisition of cloud computing services, including access, security, and reporting requirements.

All of the above clauses and provisions will apply to the purchase of commercial items and are now included in DFARS subpart 212.3, Solicitation Provisions and Contract Clauses for the Acquisition of Commercial Items.

DoD is presently soliciting comments from "small entities" concerning the impact of these regulations on their business. However, in light of the statutory underpinnings and the previous DFARS provisions, large contractors should not expect to/hope to see any major changes in the final rule.

Source URL: https://www.natlawreview.com/article/dod-addresses-cybersecurity-preparedness-incident-reporting-and-cloud-computing