KING & SPALDING

Client Alert

Privacy & Information Security – Government Investigations Practice Group

December 3, 2013

Defense Department Issues Final Rule Requiring Safeguards For Unclassified Technical Information And Cyber Incident Reporting

On November 18, 2013, the Department of Defense (DOD) published a Final Rule amending the Defense Federal Acquisition Regulation Supplement (DFARS). The new rule, which is effective immediately, is likely to have broad implications for defense contractors and subcontractors. It sets forth two new requirements.

First, the Final Rule requires government contractors to "provide adequate security" for technology systems "that *may* have unclassified controlled technical information [UCTI] *resident on or transiting through them*."[1] Without a separate system for UCTI, the rule is likely to apply to the contractor's entire network. *Second*, the Rule requires contractors to report promptly to DOD a broad range of "cyber incidents,"[2] which includes the "*possible* exfiltration, manipulation, or other loss or compromise of any unclassified controlled technical information resident on or transiting through Contractor's, or its subcontractors', unclassified information systems."[3] According to the Final Rule, these new requirements will be set forth in a specific clause in every DOD solicitation, contract, and subcontract, including those involving commercial items.

Background & Definitions

The Final Rule, which has been a work in progress since at least 2010, represents a significant expansion of the private sector's obligation to protect unclassified DOD information and report the possible loss or compromise of such information. Until now, DFARS had no provisions regarding "the safeguarding of unclassified DOD information within industry, nor . . . cyber intrusion reporting for that information."[4] DOD issued its Proposed Rule in June 2011, and received a large number of public comments. DOD modified the Proposed Rule in significant ways, which clarified many of the provisions on which industry members had commented. However, a number of provisions were not modified despite comments and complaints from industry. Some of the provisions that most concerned industry members are discussed below.

The Rule introduces various cybersecurity protection and reporting requirements on UCTI. Notwithstanding an ongoing government-wide effort to harmonize treatment of controlled unclassified information, the new rule

For more information, contact:

Eleanor Hill
+1 202 626 2955
ehill@kslaw.com

John Richter
+1 202 626 5617
jrichter@kslaw.com

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

John Drennan
+1 202 626 9605
jdrennan@kslaw.com

Clint Long
+1 202 626 2622
clong@kslaw.com

King & Spalding
Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

www.kslaw.com

contains its own definition of "UCTI" and defines "UCTI" broadly. Consequently, defense contractors and subcontractors now have an enhanced obligation to protect a number of categories of technical information such as "research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code."[5]

The Requirement to Provide "Adequate Security" – Cybersecurity Protections

As to the contractor's duty to provide "adequate security," the Final Rule imposes standards for authentication, training, incident response, contingency planning, and access controls, among others, drawn from National Institute of Standards and Technology (NIST) Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."[6] These cybersecurity protections apply to "controlled technical information," which includes "technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination."[7] Specifically, citing various sections of this NIST publication, Table 1 of Rule lists a series of "minimum security controls for safeguarding" UTCI. Defense contractors must implement these minimum requirements in their "project, enterprise, or company-wide unclassified information technology system(s) that *may* have [UCTI] resident on *or transiting through them*."[8] Without a wholly segregated information technology system for UCTI, this rule would appear to apply to a contractor's entire network. Contractors must "identify which information must be protected."[9]

If a contractor does not implement a required control, it must explain in writing to the relevant government contracting officer how either the control is not applicable or an alternative measure is being used to achieve "equivalent protection."[10] Moreover, when a contractor "reasonably determines that information systems security measures" beyond these minimum standard "may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability," the Rule obligates the contractor to apply any such other security requirements.[11] Significantly, contractors are "responsible for ensuring that the subcontractor complies with the requirements of this rule . . . ."[12]

Required Cyber Incident Reporting and Cooperation In DOD Damage Assessments

With promulgation of the Final Rule, defense contractors are obliged to report certain cyber incidents to DOD within 72 hours of discovery. Reportable cyber incidents include those "involving *possible* exfiltration, manipulation, or other loss or compromise of any [UCTI] resident on or transiting through Contractor's, *or its subcontractors'*, unclassified information systems" and "[a]ny other activities . . . that allow unauthorized access to the Contractor's unclassified information system on which [UCTI] is resident on or transiting."[13]

Within the 72-hour period, the Rule requires contractors to provide "as much … information as can be obtained" to DOD in multiple areas. These areas include the location of incident; the name of subcontractor if not on the prime contractor network; the contract clearance level; the DOD programs, platforms or systems involved; the date the incident was discovered; the type of compromise; and a description of the technical information compromised. Beyond the initial reporting requirements, the Final Rule also imposes duties on the contracting community to support DOD damage assessments. A reportable cyber incident triggers an obligation on the part of the contractor to conduct further review of its unclassified network for evidence of compromise resulting from a cyber incident to include, but is not

limited to, identifying compromised computers, servers, specific data and users accounts. Contractors must analyze the compromised information system as well as other information systems on the network that were accessed as a result of the compromise. In addition, contractors must review the data accessed during the cyber incident to identify specific UCTI associated with DOD programs, systems or contracts, including military programs, systems and technology.

Finally, contractors must preserve and protect images of known affected information systems and all relevant monitoring and packet capture data for at least 90 days from the cyber incident to allow DOD to request information or decline interest. Moreover, additional obligations are imposed on the contractor where DOD elects to conduct a damage assessment including a requirement to share files and images unless there are legal restrictions that limit the ability to share digital media.

Contractors should be aware of a few key implications and provisions of this reporting requirement:

- *First*, cyber incidents trigger the reporting requirement even without adverse effects because the Final Rule defines cyber incident to include actions that result in a "*potentially* adverse effect on an information system and/or the information residing therein."[14] Moreover, a cyber incident can be something as simple (but serious) as "the copying of data to unauthorized media."[15]

- *Second*, contractors must report relevant cyber incidents involving their subcontractors' systems. Indeed, DOD's response to Comment 29 makes it clear that prime contractors must "report when [UCTI] has potentially been compromised regardless of whether the incident occurred on a prime contractor's information system or on a subcontractor's information system."

- *Third*, the implications of reporting a cyber incident are not clear. To be sure, the Rule provides that a "cyber incident that is *properly reported* by the contractor shall not, *by itself*, be interpreted under this clause as evidence that the contractor has failed to provide adequate information safeguards . . ."[16] Contractors also should be aware, however, that DOD "does not intend to provide any safe harbor statements" in connection with reportable cyber incidents.[17] It is not clear what other factors, beyond the mere occurrence of a cyber incident that is properly reported, will impact DOD's assessment of contractor compliance with the requirement to provide adequate security measures.

- *Finally*, contractors should note that the contracting officer has discretion to conduct audits and reviews of contractors' safeguarding measures "in accordance with the terms of the contract."[18] It is therefore possible that defense contractors may face audit and investigation costs before and after a cyber incident.

Recommendations

The Final Rule became effective as on November 18, 2013, and requires, at bottom, that contractors provide "adequate security to safeguard" UCTI. Contractors must recognize that they have the burden of determining what information is protected, which means that they should be familiar with the definition of UCTI and the "adequate security" requirements. In response to industry comments, DOD also said that "[t]he rule does not require a specific analysis to determine if additional controls are required. The intent is to require that if the contractor is aware, based on an already

assessed risk or vulnerability that the specified controls are inadequate, then the contractor must implement additional controls to mitigate the specific shortcoming."[19] Furthermore, contractors must be prepared to identify and report cyber incidents involving UCTI in their systems and their subcontractors' systems.

Additionally, it is clear that contractors are responsible for subcontractors' compliance with these security requirements and for reporting cyber incidents involving subcontractors' systems. Therefore, contractors should actively participate with their subcontractors—which includes Internet Service Providers or cloud service providers per DOD's Response to Comment 3—in order to ensure compliance with the Final Rule and to promptly report any relevant cyber incidents. Moreover, it would be prudent for contractors to examine their contractual rights to: (i) audit subcontractors' network security safeguards; (ii) require subcontractors to notify the contractor of any cyber incidents; and (iii) participate in any investigation related to a cyber incident involving a subcontractor's network.

While immediate compliance is required, DOD's response to Comment 14 states that "[i]mplementation of the rule does not direct modification of existing contracts." As to the cost of compliance, DOD's response to Comment 10 notes that "costs associated with implementation will be allowable and chargeable to indirect cost pools" but that the "Government does not intend to directly pay for the operating costs associated with the rule." Moreover, in its response to Comment 7, DOD advised that "[i]mplementation of this rule may increase contractor costs that would be accounted for through the normal course of business."

King & Spalding is particularly well-equipped to assist clients in the defense, intelligence, and national security arenas. Our team includes lawyers with years of experience handling highly sensitive, and often classified, national security issues, at very senior levels, in both government and the private sector. The firm's government investigations practice, for example, includes a former Deputy Attorney General, a former Department of Defense Inspector General, other senior Department of Justice and SEC officials, numerous former federal prosecutors, and the Staff Director of the House and Senate Intelligence Committees' Joint Inquiry on the September 11th Attacks. Both the firm's government investigations and government relations practices are consistently recognized by Chambers USA as among the best in the United States.

Similarly, our Privacy & Information Security Practice has unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents, interfacing with stakeholders and the government, engaging in complex civil litigation (such as class actions), handling state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of state and federal government.

In short, King & Spalding lawyers have represented and assisted major defense contractors in connection with the new legal requirement posed by the Final Rule on protecting UCTI.

If you have any questions regarding the updated DOD regulations or related issues, please contact Eleanor Hill at +1 202 626 2955, John Richter at +1 202 626 5617, Alexander Haas at +1 202 626 5502, John Drennan at +1 202 626 9605, or Clint Long at +1 202 626 2622.

---

[1] *Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039)*, 78 Fed. Reg. 69273, 69280, 69282 (Nov. 18, 2013) ("Final Rule"); *see also* 48 C.F.R. §§ 252.205-7012(b)(1) (2013). (emphases added).
[2] Final Rule, 78 Fed. Reg. at 69282; *see also* 48 C.F.R. § 252.204-7012(d)(1)-(2).
[3] Final Rule, 78 Fed. Reg. at 69280; *see also* 48 C.F.R. § 252.204-7012(a).
[4] *Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039)*, 76 Fed. Reg. 38089, 38089 (June 29, 2011) ("Proposed Rule").
[5] Final Rule, 78 Fed. Reg. at 69280; *see also* 48 C.F.R. § 252.204-7012(a).
[6] Final Rule, 78 Fed. Reg. at 69280; *see also* 48 C.F.R. § 252.204-7012(b)(1)(i).
[7] Final Rule, 78 Fed. Reg. at 69280; *see also* 48 C.F.R. § 252.204-7012(a).
[8] Final Rule, 78 Fed. Reg. at 69280; *see also* 48 C.F.R. § 252.204-7012(b)(1) (emphases added).
[9] Final Rule, 78 Fed. Reg. at 69276.
[10] Final Rule, 78 Fed. Reg. at 69280; *see also* 48 C.F.R. § 252.204-7012(b)(1)(ii).
[11] Final Rule, 78 Fed. Reg. at 69280; *see also* 48 C.F.R. § 252.204-7012(b)(2).
[12] *Id.* at 69274.
[13] Final Rule, 78 Fed. Reg. at 69282; *see also* 48 C.F.R. § 252.204-7012(d)(2) (emphases added).
[14] Final Rule, 78 Fed. Reg. at 69280; *see also* 48 C.F.R. § 252.204-7012(a).
[15] *Id.*
[16] Final Rule, 78 Fed. Reg. at 69280; *see also* 48 C.F.R. § 204.7302(b)(2) (emphases added).
[17] *Id.* at 69277–78.
[18] Final Rule, 78 Fed. Reg. at 69274.
[19] *Id.* at 69276.