KING & SPALDING

Client Alert

National Security, Intelligence & Defense – Data, Privacy & Security Practice Group

August 27, 2015

Defense Department Issues Interim Rule Requiring Contractor and Subcontractor Reporting of Cyber Incidents

On August 26, 2015, the Department of Defense (DoD) published a long-awaited Interim Rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to require "rapid" reporting of "cyber incidents" that result in an "actual or potentially adverse effect" on certain information systems or defense information residing on contractor networks. The Interim Rule is effective immediately; a copy from the Federal Register is available **here**.

Executive Summary

The Interim Rule results in a significant expansion of the mandate on defense contractors and their subcontractors to report on network penetrations and other cyber incidents. Not only does the Interim Rule expand the class of information covered by these new reporting requirements beyond controlled technical information, the Interim Rule also expands coverage to any cyber incident on a covered defense contractor's system and modifies the baseline of what types of cybersecurity measures constitute adequate security. DoD has also included a host of new contract clauses delineating these requirements that explicitly require flowing these security and reporting requirements down to subcontractors and lower-tier contractors.

DoD took the unusual step of issuing an Interim Rule without first issuing a Proposed Rule for comment in view of "the urgent need to protect covered defense information and gain awareness of the full scope of cyber incidents being committed against defense contractors." DoD noted the "proliferation of information technology and increased information access allowed by cloud computing environments has also increased the vulnerability of DoD information via attacks on its systems and networks and those of DoD contractors," as a reason to not issue a Proposed Rule. The new rule is likely to have broad implications for defense contractors and subcontractors and has four principal impacts.

First, the Interim Rule expands a contractor's safeguarding and reporting duties to require protection of "covered defense information," which includes controlled technical information, export controlled information, critical information, and other information requiring protection by law, regulation, or government-wide policy.

For more information, contact:

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

Gary G. Grindler
+1 202 626 5509
ggrindler@kslaw.com

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

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

Nicholas A. Oldham
+1 202 626 3740
noldham@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

Second, the Interim Rule now requires contractors to report "cyber incidents" involving this new class of information on entire covered contractor systems as well as "*any* cyber incident that *may* affect the ability to provide operationally critical support."

Third, the Interim Rule modifies the baseline cybersecurity standards defense contractors must comply with to provide "adequate security" by referencing a different NIST publication.

Fourth, the Interim Rule implements DoD policies to ensure uniform application of DoD policies and procedures when contracting for cloud services across DoD. Specifically, the Interim Rule codifies and expands on prior policy memoranda issued by its Chief Information Officer (CIO) in the past year.

DoD stated that these requirements "will serve to increase the cyber security requirements placed on DoD information in contractor systems and will help the DoD to mitigate the risks related to compromised information as well as gather information for future improvements in cyber security policy."

Expansion of Required Cyber Incident Reporting

The Interim Rule is not a bolt out of the blue. It has been in progress since 2013 and represents a significant, but anticipated, expansion of the private sector's obligation to protect unclassified DoD information and report the possible loss or compromise of such information. The Interim Rule implements requirements of Section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 (Pub. L. 112-239), Section 1632 of the NDAA for FY 2015, and DoD CIO policy for the acquisition of cloud computing services.

Until now, DFARS required cyber incident reporting for Unclassified Controlled Technical Information (UCTI), but did not require such reporting for other unclassified information. The Interim Rule changes that by extending the reporting and other cybersecurity protection requirements to "covered defense information," defined as unclassified information that is "Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract" that falls into one of four categories: "(i) Controlled technical information; (ii) Critical information (operations security); (iii) Export control information; or (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)."

At the same time, the Interim Rule also defines "cyber incident" more broadly than network penetrations or the exfiltration of data. "Cyber incident" includes any "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." The Interim Rule likewise defines "compromise" broadly to mean the "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."

The Interim Rule additionally includes new clauses that must be included in contracts. These clauses require cyber incident reporting when the contractor "discovers a cyber incident that affects a covered contractor information system *or* the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support." The requirement to include these new contract clauses is a significant expansion of prior DFARS requirements. Under the Interim Rule, defense contractors that learn of a cyber incident are obligated to conduct a review for evidence of compromise of covered defense information, "including, but not limited to, identifying compromised computers, servers, specific data, and user accounts" and "analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident

in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support."

The Interim Rule further requires contractors to "rapidly report" cyber incidents to DoD. This generally means that such reporting must occur within 72 hours of discovery of the cyber incident. To this end, contractors must "have or acquire a DoD-approved medium assurance certificate." For information on obtaining a DoD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/certificate.html. Contractors are required to "preserve and protect images of all known affected information systems" and "all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest." These requirements will often mean that contractors must promptly engage forensic experts to ensure that data is retained and preserved. Further, DoD can require the contractor to provide access to additional information or equipment necessary for forensic analysis and require cyber incident damage assessment activities to assist DoD.

Moreover, prime contractors are now required to "include the substance" of these contract clauses "in all subcontracts for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, *including subcontracts for commercial items*." The Interim Rule also explicitly requires subcontractors of prime DoD contractors "to rapidly report cyber incidents directly to DoD" through the dibnet portal (http://dibnet.DoD.mil) as well as reports the prime contractor. Similarly, "[l]ower-tier subcontractors are required to likewise report the same information to their higher-tier subcontractor, until the prime contractor is reached."

In short, defense contractors and subcontractors now have an enhanced obligation to protect a number of categories of unclassified information and to report cyber incidents to DoD.

Contractors should be aware of a few key implications and provisions of these reporting requirements:

- Cyber incidents trigger the reporting requirement even without adverse effects because the Interim Rule defines cyber incident to include actions that result in a "*potentially* adverse effect on an information system and/or the information residing therein." When paired with the definition of "compromise," a large swath of cyber incidents are covered that would not necessarily involve a network penetration or the known exfiltration of data.

- Contractors must report relevant cyber incidents involving their subcontractors' systems and must be prepared for subcontractors and lower-tier subcontractors to report information to DoD before the prime contractor learns of the possible cyber incident.

- The implications of reporting a cyber incident are unclear. To be sure, the Interim Rule provides that a "cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate information safeguards for covered defense information on their unclassified information systems." But DoD has previously stated that it does not intend to provide safe-harbor statements related to reportable cyber incidents. It is not yet clear what other factors, beyond the mere occurrence of a properly reported cyber incident, will impact DoD's assessment of contractor compliance with the requirement to provide adequate security measures.

- Contractors should be aware DoD has substantial authority to use information provided in cyber incident reports, including "contractor attributional/proprietary information not created by or for DoD." DoD may release this information: (1) to entities with missions that may be affected by such information; (2) to entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents; (3) to Government entities that conduct counterintelligence or law enforcement investigations; (4) for national

security purposes, including cyber situational awareness and defense purposes; or (5) to certain support services contractor under particular government contracts.

Modifying the Requirement to Provide "Adequate Security" – Updated Cybersecurity Protections

The Interim Rule requires contractors to provide "adequate security" for covered defense information. The Interim Rule also modifies DOD's understanding of minimum cybersecurity protections. Previously, DOD had imposed standards for authentication, training, incident response, contingency planning, and access controls, among others, by drawing from National Institute of Standards and Technology (NIST) **Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations**." The Interim Rule replaces these requirements with a requirement to follow a different set of NIST controls, namely, **NIST SP 800-171, entitled "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations**." NIST SP 800-171, finalized by NIST in June 2015, is specifically for protecting sensitive information that resides in contractor information systems. NIST SP 800-171 also refines the requirements of Federal Information Processing Standard (FIPS) 200 and the controls of NIST SP 800-53. DoD concluded in the Interim Rule that this new standard is "easier to use" and "greatly increases the protections of Government information in contractor information systems, while simultaneously reducing the burden placed on the contractor by eliminating Federal-centric processes and requirements."

Defense contractors may obtain variances from contracting officers in advance, but they must otherwise implement these minimum requirements in their unclassified information technology systems that could have covered defense information resident on them or transiting through them. Without a wholly segregated information technology system for covered defense information, this rule would appear to apply to a contractor's entire network.

Cloud Computing Requirements

This Interim Rule also implements DoD policies and procedures for use when contracting for cloud computing services. In December 2014, the DoD CIO issued a memo to clarify DoD guidance when acquiring commercial cloud services. *See* "**Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services**". In January 2015, the DoD CIO issued guidance for cloud service providers to comply with when providing the DoD with cloud services. *See* **Cloud Computing Security Requirements Guide (SRG)** Version 1, Release 1 on January 13, 2015. The Interim Rule implements these new policies to ensure uniform application when contracting for cloud services across DOD.

Under the Interim Rule DoD shall acquire cloud computing services using commercial terms and conditions that are consistent with Federal law, and an agency's needs, including those requirements specified in this subpart. Some examples of commercial terms and conditions are license agreements, End User License Agreements (EULAs), Terms of Service (TOS), or other similar legal instruments or agreements.

Interestingly, DoD wades into the debate about the physical location of data stored in the cloud environment by requiring cloud-computing service providers "to maintain within the 50 states, the District of Columbia, or outlying areas of the United States, all Government data that is not physically located on DoD premises." Cloud-computing service providers and users of cloud-computing services under DoD contracts are all required to report cyber incidents in a manner consistent with the other portions of the Interim Rule.

Recommendations

The Interim Rule became effective when it was published on August 26, 2015. DoD will be accepting comments on the Interim Rule for 60-days, or until October 26, 2015. We recommend that contractors subject to the Interim Rule

carefully consider the expanded requirements and burdens imposed by the Interim Rule. Covered defense contractors and subcontractors may also wish to submit comments on the Interim Rule to DoD.

As noted, the Interim Rule requires that contractors provide adequate security to safeguard "covered defense information" under NIST standards and report on cyber incidents, which is broadly defined. Contractors should recognize that their reporting obligations have been significantly expanded under the Interim Rule and that they have the burden of determining what information is protected, what systems are covered, and what constitutes a "cyber incident." The Interim Rule also changes the applicable baseline security standards by requiring contractors to apply standards from NIST SP 800-171. Contractors should move quickly to ensure that their security practices comply with this new standard.

The duties imposed by the Interim Rule flow down to subcontractors and reporting requirements flow up to prime contractors, meaning that defense contractors must be prepared to identify and report cyber incidents in their systems and their subcontractors' systems. As a result, contractors must actively participate with subcontractors to ensure compliance with the Interim 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 subcontractors' network.

Finally, we believe it is likely that future audits by the DoD Inspector General, other Inspectors General, or investigations by Congress could well result from reported cyber incidents. Companies subject to these new rules should act accordingly and take care to regularly examine their governance and compliance regimes and work with outside counsel and experts in advance of a reportable cyber incident.

King & Spalding is particularly well-equipped to assist clients with our **National Security, Intelligence, and Defense Industry Practice**. 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 acting 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 **Data, Privacy & Security Practice** has unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents including data breaches and cybersecurity 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.

If you have any questions regarding the updated DoD regulations or related issues, please contact **Eleanor J. Hill** at +1 202 626-2955, **Gary G. Grindler** at +1 202 626-5509, **Alexander K. Haas** at +1 202 626-5502, **John A. Drennan** at +1 202 626-9605, or **Nicholas A. Oldham** at +1 202 626-3740.