WILMERHALE

Department of Defense Revises Landmark Cybersecurity Rule, Extends Deadline for Some Compliance Requirements

JANUARY 8, 2016

On December 30, 2015, the Department of Defense (DoD) issued a second interim rule on *Network Penetration Reporting and Contracting for Cloud Services*,[1] amending an earlier version issued on August 26, 2015.[2] The new, amended DoD interim rule prescribes cybersecurity requirements, including mandatory cybersecurity-related contract clauses in all DoD contracts subject to the Defense Federal Acquisition Regulations Supplement (DFARS). Despite its narrow title, the rule remains expansive in scope and prescriptive in application, mandating specific data security controls for sensitive unclassified information throughout the DoD supply chain. As such, the rule, even as revised, will affect both Defense Industrial Base (DIB) and other companies.

The new, amended interim rule addresses the following principal topics:

- **Cybersecurity Standards for Handling Covered Defense Information on Company Systems**. Contractors that process, store, or transit "Covered Defense Information" (CDI) will have until December 31, 2017 to attain compliance with all of the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*.[3] To the extent a contractor is not in compliance with a NIST SP 800-171 provision between now and December 31, 2017, the contractor must notify DoD about which security requirements are not currently in place.[4]

  Even with the extended deadline of December 2017, companies may still find it challenging to update legacy systems and otherwise comply with all requirements of NIST SP 800-171.

- **Cybersecurity Standards for Providing Cloud or Other IT Services to DoD**. The new rule separately establishes minimum security requirements for the provision of IT support or cloud computing services to DoD. The rule requires, among other things, that all cloud computing services implement controls in accordance with the DoD Cloud Computing Security Requirements Guide.

- **Cyber Incident Reporting Requirements**. Contractors must rapidly report (within 72 hours

of discovery) cyber incidents affecting covered contractor information systems,[5] CDI, or the contractor's ability to perform requirements of a contract designated as “operationally critical support.” Note that this requirement will be immediately applicable to contracts and implementation is not delayed until December 2017.

- **Contract Clauses Must Be Flowed Down to Subcontractors Handling CDI**. The new, amended rule's contract clauses must be flowed down to only those subcontractors whose “efforts will involve” CDI or where subcontractors will provide operationally critical support.[6] In contrast, the original interim rule required the clauses be flowed down to all subcontractors at all tiers.

The new interim rule followed a period of intense opposition from defense contractors and industry groups objecting to the scope of the initial rule, especially the original requirement that contractors' internal networks immediately comply with NIST SP 800-171 standards.

DoD is accepting comments on the new, amended interim rule through February 29, 2016. Further explanation of the rule, including background information about the origin of the various requirements, is provided below.

Background: Putting the New Rule in Context

In the face of growing cyber threats, the Obama Administration and Congress have taken a number of steps aimed at securing information held by DIB companies.

- **Defense Authorization Acts Mandate Rulemaking on Incident Reporting**. The National Defense Authorization Acts (NDAAs) for fiscal years (FY) 2013 and 2015, and the Intelligence Authorization Act of 2014, mandated that DoD and the Office of the Director of National Intelligence (ODNI) each issue rules requiring contractor breach reporting.[7] These mandates, however, only applied to specific categories of contractors: “cleared defense contractors,” “operationally critical contractors,” and “cleared intelligence contractors.”[8]

- **DoD Issues Final “UCTI” Rule**. In November 2013, DoD published a final rule, requiring contractors (1) to satisfy security standards described in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*,[9] in order to protect “unclassified controlled technical information” (UCTI)[10] and (2) to report to DoD cyber incidents that affected UCTI.[11]

- **DoD-GSA Working Group Issue Recommendations**. In January 2014, pursuant to a mandate in President Obama's February 2013 executive order on critical infrastructure cybersecurity, a General Services Administration (GSA) and DoD joint working group published recommendations on “incorporating security standards into acquisition planning and contract administration.”[12] The report noted that “implementing these recommendations may contribute to increases in cybersecurity across the broader economy.”[13]

- **The August 2015 Interim Network Penetration Rule**. Against this backdrop, DoD issued the August 2015 interim rule, which greatly expanded the UCTI rule beyond any of the NDAA rulemaking requirements. Since promulgating the August rule (which took effect immediately), DoD has provided guidance in several forums. Most significantly, DoD (1) issued a Frequently Asked Questions (FAQ) document on November 17, 2015;[14] (2) published updated Procedures, Guidance, and Information (PGI) the following day;[15] and (3) held a public meeting on the rule on December 14, 2015.[16]

The New, Amended Rule and DoD Guidance

DoD's stated purpose in issuing the new, amended rule in December 2015 was to implement the rapid reporting cyber incident requirements from the FY 2013 and 2015 NDAAs, covering cleared defense contractors and operationally critical contractors, as well as the DoD cloud computing services policies and procedures. However, the rule applies to all DoD contractors (including providers of commercial supplies and services) and is not limited to cleared or operationally critical contractors.

Like the 2013 UCTI rule, the rule includes two primary components: (1) network security controls and (2) cybersecurity incident reporting.

These requirements apply to “Covered Defense Information” (CDI), a term that is defined broadly to cover a large swath of information that may be maintained by DoD contractors and subcontractors, commercial or otherwise, at all tiers. Specifically, the term is 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 is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract, and falls under one of four categories:

- controlled technical information;
- critical information for operations security;
- export controlled information; or
- any other information, marked or identified in the contract, that otherwise requires safeguarding or dissemination controls (e.g., proprietary business information or information protected under the Privacy Act).

Note that this definition of CDI potentially covers a significant amount of information and such information may not be easily identified by written markings. While Contracting Officers (COs) are supposed to designate whether CDI is expected to be provided or generated in the contract, contractors are required to comply with the rule's requirements if they determine that they are generating or using CDI during performance, even in the absence of a contractual designation.

While the original interim rule required the contract clauses be included in subcontracts at all tiers, the second interim rule amended the flowdown requirement to require inclusion of the clause only

to subcontractors whose “efforts will involve” CDI or that will provide operationally critical support. However, because of the breadth of the definition of CDI, the flowdown requirement may nevertheless reach many subcontractors.

Network Security Controls

Under the interim rule, contractors are required to safeguard CDI by applying network security controls. In general, the rule requires all contractors to provide “adequate security,” meaning they apply protective measures that are commensurate with the consequences and probability of loss, misuse, unauthorized access to, or modification of information. The meaning of “adequate security” varies depending on the type of contract or system at issue.

- For contractor's internal systems that are processing, storing, or transiting CDI, contractors are required to, at a minimum, meet the security requirements in NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, using the version in effect at the time the solicitation is issued or as authorized by the CO. For those contracts issued with the clause as amended, all controls are required to be implemented “as soon as practical,” but no later than December 31, 2017. Until then, contractors must provide notice to DoD within 30 days of award if any NIST SP 800-171 security requirements are not met.

  If contractors cannot meet all of the requirements, they can employ alternate equally effective measures only if a representative of the DoD Chief Information Officer (CIO) provides written acceptance of the alternative control.[17]

- For IT systems or services (other than cloud services) operated for the government, contractors are required to comply with security requirements specified in the contract. While unstated in the rule, DoD stated in the December 14 meeting that the applicable controls will reflect Committee on National Security Systems Instructions No. 1253, *Security Categorization and Control Selection for National Security Systems*,[18] which, in turn, are based on NIST SP 800-53 (the NIST publication used in the UCTI rule).

- Finally, for cloud services operated for the government, contractors shall implement safeguards in accordance with the DoD Cloud Computing Security Requirements Guide.[19] Cloud providers are also required to maintain the data within the US, unless the CIO provides written notification to use another location.

Contractors are required to “[a]pply other security measures when the Contractor reasonably determines that such measures, in addition to those identified [above], may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.”

Cybersecurity Incident Reporting

Contractors must rapidly report (within 72 hours of discovery) cyber incidents affecting covered information systems, CDI, or the contractor's ability to perform requirements of a contract

designated as “operationally critical support.”[20] What constitutes a “compromise” under the rule is not clear, and DoD CIO representatives at the public meeting urged contractors to use their judgment. Contractors are required to submit malware samples, and preserve system images and monitoring data for 90 days. Upon request, the contractor shall provide DoD access to information and equipment.

Looking Forward

In light of the rule's breadth and scope, the rule is already having a significant impact on many contractors. As more contracts are issued with these new contract clauses, the burden throughout the supply chain will only increase.

- **Supply Chain Issues**. While the security and incident reporting requirements may more readily be met by large prime contractors whose implementation costs are spread across substantial DoD business, the rule appears likely to be burdensome and possibly cost prohibitive for many key suppliers, particularly those without substantial DoD business. DoD's outreach regarding the rule has focused almost exclusively on its DIB partners, leaving the DIB with the burden of conducting outreach to subcontractors that may be small companies or may primarily service non-defense commercial customers. During the public meeting, DoD committed to utilizing its traditional avenues for small business outreach, but ultimately suggested that prime contractors should think creatively to promote subcontractor compliance. While the second interim rule provides additional time for continued outreach, prime contractors will likely continue to bear the primary burden for subcontractor compliance, particularly in coordinating subcontractors' reports on any gaps in the implementation of required security controls.

- **Compliance and Enforcement**. As DoD made clear in its FAQ, the new rule did not add any new compliance monitoring mechanisms. Instead, compliance is “subject to any existing generally applicable contractor compliance monitoring mechanism.” Thus, contractors failing to comply with the rule could be subject to liability under existing laws and regulations, such as the False Claims Act.

- **Interaction with Intelligence Community Rulemaking**. Although ODNI has not yet issued the incident reporting requirements mandated by Congress, DoD has coordinated with ODNI so that contractors working for both DoD and intelligence agencies can report incidents through the DoD portal. It remains to be seen whether ODNI will adopt other aspects of the DFARS rule.

- **Rules on Liability Protection**. With few changes, the FY 2016 NDAA codified the relevant cybersecurity provisions from the 2013 NDAA, but it also added new liability protection for information-sharing between defense contractors and DoD,[21] to be implemented in a separate rulemaking.

For more information on cybersecurity for government contractors, view the recording and materials

from the recent installment of our Cybersecurity, Privacy and Communications Webinar Series: Recent Data Security Developments for Government Contractors, here.

[1] 80 Fed. Reg. 81472 (Dec. 30, 2015), available here.

[2] 80 Fed. Reg. 51739 (Aug. 26, 2015), available here.

[3] NIST SP 800-171 is available here.

[4] For those companies who received a contract prior to December 30, 2015 and thus potentially subject to the August 2015 rule, they should review the contract and consider seeking appropriate modifications to the contract if the company wants to clarify that the newly released revised December 2015 interim rule provides the applicable cyber requirements for the contract. Note that under the August 2015 rule, the security requirements are required to be implemented immediately upon award, unless an alternative control (or a statement that the control does not apply) is approved by DoD Chief Information Officer. However, DoD did issue a class deviation for one of the most onerous requirements, allowing contractors (with notice to DoD) to take up to nine months from contract award to implement multi-factor authentication. Class Deviation 2016-O001, Memorandum from Claire M. Grady, Director, Defense Procurement and Acquisition Policy (Oct. 8, 2015), available here.

[5] A "covered contractor information system" is defined as "an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits [CDI]." 80 Fed. Reg. 51742 (adding definition to 48 C.F.R. 204.7301).

[6] 80 Fed. Reg. 81474 (revising 48 C.F.R. 252.204-7012(m)(1)).

[7] National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-329 (NDAA 2013), Section 941; Carl Leven and Howard P. "Buck" McKeon National defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291 (NDAA 2015), Section 1632; Intelligence Authorization Act of 2014 (IAA 2014), Pub. L. No. 113-126, Section 325. For more information on Section 941 of the 2013 NDAA, see our previous alert, available here.

[8] "Cleared defense contractors" are private entities granted clearance by DoD to "access, receive, or store classified information" for contract bids or activities supporting DoD programs. NDAA 2013, Section 941(e)(1). "Operationally critical contractors" is narrowly defined as a contractor designated as a critical source of supply for certain transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forced. NDAA 2015, Section 1632. "Cleared intelligence contractors" is defined similarly to "cleared defense contractors," but supporting a program of an element of the intelligence community. IAA 2014, Section 325(f)(1).

[9] NIST SP 800-53 is available here.

[10] The rule defined UCTI as computer software or technical data with military or space application that is subject to controls on access, use, reproduction, modification, performance, display, release,

disclosure, or dissemination, and that is marked as controlled information pursuant to DoD rules. Examples of technical information that could be specially marked as UCTI include “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."

[11] 78 Fed. Reg. 69273 (Nov. 18, 2013), available here. For more information on the “UCTI Rule,” see our previous alert, available here, and Benjamin Powell, et al, "What You Should Know About DoD's Cybersecurity Rule," Law360 (Nov. 25, 2013), available here.

[12] “Improving Cybersecurity and Resilience Through Acquisition,” prefaced by a memorandum from Chuck Hagel, Secretary of Defense and Daniel M. Tangherlini, Administrator of General Services, to the Assistant to the President for Homeland Security and Assistant to the President for Economic Affairs (Jan. 23, 2014), available here. For more information on this report, see our previous alert, available here.

[13] Id. at 9.

[14] Defense Procurement and Acquisition Policy, Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73, DFARS Subpart 239.76 and PGI Subpart 239.76, Class Deviation 2016-O0001 (OCT 2015) (Nov. 17, 2015), available here.

[15] DFARS Procedures, Guidance, and Information, Subparts 204.73 and 239.76 (rev. Nov. 18, 2015), available here and here.

[16] 80 Fed. Reg. 72712 (Nov. 20, 2015), available here; slides from presentation available here.

[17] The first interim rule provided that the DoD CIO representative would approve or disapprove of the request prior to award, and that the approved deviation would be incorporated into the resulting contract. This requirement was removed in the second interim rule.

[18] CNSSI No. 1253 is available here.

[19] The DoD Cloud Computing Security Requirements Guide is available here.

[20] While not apparent from the face of the rule, during the December 14 meeting, DoD representatives stated that the only requirement with respect to a compromise affecting “operationally critical support” (as distinguished from “critical information (operations security),” a category of CDI) is to report a cyber incident that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support.

[21] See National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, Section 1641(a).

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195