Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Watch Out For New Cybersecurity Rules, Defense Contractors

Law360, New York (March 01, 2013, 1:21 PM ET) -- The clock is ticking for the U.S. Department of Defense to establish "rapid reporting" requirements for cleared defense contractors to report cyber intrusions on their networks. Section 941 of the National Defense Authorization Act for 2013, signed by the president on Jan. 2, 2013, mandates that the secretary of defense establish such reporting procedures within 90 days of the act.[1]

While Section 941 sets out a basic framework for what the new procedures must require, it leaves unresolved several open questions as to how the DOD will implement the new rapid reporting requirements. On Jan. 31, 2013, the Defense Acquisition Regulations Council opened a new Defense Federal Acquisition Regulation Supplement case, 2013-D018, Reports to DOD on Penetrations of Networks and Information Systems, to implement Section 941. Contractors should be on alert for a forthcoming rulemaking notice, which would include an opportunity for public comments.

Overview of the Section 941 Requirements

The Section 941 requirements apply to cleared defense contractors, which include any company granted clearance by the DOD to access, receive or store classified information for the purpose of bidding for a contract or conducting other activities in support of a DOD program.[2] Covered networks mean any network or information of a cleared defense contractor that contains or processes DOD information and to which the cleared contractor must apply enhanced protection. Section 941 requires the secretary of defense to designate a senior official to establish criteria for covered networks to be subject to the new reporting procedures.[3]

The forthcoming procedures will require that, in the event of a successful penetration of a cleared defense contractor's covered network, the contractor must rapidly report to the DOD a description of the method used to penetrate the network, including a sample of any malicious software identified, and a summary of DOD information that may have been compromised.[4]

In addition, the forthcoming procedures must provide a mechanism for DOD personnel to gain access to a contractor's equipment or information for the DOD to conduct forensic analysis of the penetration. Section 941 limits the DOD's access to what is necessary to determine whether DOD information "was successfully exfiltrated," and if so, to determine what DOD information was compromised.

Further, the access procedures are to "provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person."[5] The statute also provides that the forthcoming procedures shall prohibit the dissemination outside the DOD of information obtained or derived through such procedures that is not DOD information except with the contractor's approval.[6]

Section 941 affords the DOD substantial discretion in implementing the new rapid reporting procedures. There are several areas of interest that may be important to contractors subject to these new reporting requirements.

Interaction with Existing and Proposed Disclosure Mechanisms

The new reporting procedures under Section 941 are intended to coexist with and build upon already existing DOD mechanisms to combat cyber intrusions. The joint statement of the managers included with the NDAA conference report advises that Section 941's requirements are "intended to be compatible with, and provide support for," a pending DFARS rulemaking aimed at safeguarding DOD information across contractor information systems and requiring reporting of cyber intrusions on unclassified contractor systems.[7] The proposed rule, aimed at a wider pool of defense contractors than just cleared contractors, sets forth detailed procedures for reporting cyber intrusions and further outlines safeguards for protecting sensitive contractor or third party information that is reported to the government.

In addition, the joint statement "encourage[s] DOD to build on the existing voluntary [Defense Industrial Base] DIB information sharing program." The voluntary DIB cybersecurity information sharing program, expanded in 2012 through an interim rulemaking, is a voluntary framework for bilateral information sharing in which DIB participants report cyber incidents to the government and the government in return shares cyber threat information and information assurance best practices with participants.[8]

The existing DFARS proposed rulemaking and the DIB voluntary cybersecurity information sharing program interim rule may provide some guidance as to what contractors can expect when DOD issues the new rapid reporting procedures.

Areas of Interest for Contractors

Further, the joint statement of the managers accompanying the NDAA conference report highlights particular areas where more DOD guidance is needed, advising the DOD to build upon the DIB information sharing program in "such areas as the definition of reportable events, and the forensic damage assessment process."[9] The forthcoming procedures in these and other areas may facilitate improved cybersecurity information-sharing between the government and industry participants, but also may present practical challenges to implement increased cybersecurity reporting standards and may heighten concerns about protection of the contractor's or third parties' sensitive or proprietary information. These areas also may represent the best opportunity for industry to help shape future cybersecurity standards as DOD develops the required reporting procedures.

Reportable Events

To the extent the DOD clarifies standards for reportable cyber intrusion events in the forthcoming procedures, it will be incumbent upon cleared defense contractors to ensure they have appropriate mechanisms in place to identify such events on their covered systems.

Forensic Damage Assessment

While Section 941 requires contractors to provide the DOD access to covered systems for the purpose of determining whether and to what extent DOD information may have been exfiltrated during a cyber intrusion, the section instructs that the access procedures must provide for the "reasonable protection" of trade secrets, commercial or financial information, and information that can be used to identify a specific person. The joint statement suggests that the access procedures should allow contractors "to remove proprietary or other types of information before DOD forensics teams copy information or 'image' systems."

It is yet to be seen how the DOD will strike the balance between its need for access to cyber intrusion information and the rights of contractors to protect their and third parties' sensitive and proprietary information. Contractors should consider what safeguards and procedures are necessary to protect sensitive information on their networks that is unrelated to identifying the scope of a cyber intrusion.

Opportunity for Public Comment

While Section 941 does not mandate that the DOD act through a rulemaking with public notice and comment, the joint statement of the managers instructs that the DOD is expected to consult with industry as it develops the reporting process.[10] The DAR Council has opened a new DFARS case, 2013-D018, Reports to DOD on Penetrations of Networks and Information Systems, to implement Section 941. The DAR Council has indicated that it may proceed through an interim rule, which would include a request for public comments. While the publication of a rulemaking would provide an opportunity for interested parties to submit comments, contractors may also want to consider commenting now in advance of the rulemaking.

Conclusion

Ultimately, per Section 941's mandate, the DOD is likely to act soon to implement the increased reporting obligations for cleared defense contractors. Further, the cybersecurity responsibilities for all defense contractors are likely to continue to increase in the future as legislative and regulatory efforts continue to develop. Contractors should be mindful that other opportunities to engage with the DOD on the development of cybersecurity procedures may occur on an informal basis. Further, as the regulatory landscape evolves, contractors may be subject to overlapping reporting regimes and will need to develop adequate practices to comply with their increased obligations.

--By Ronald D. Lee and Lauren J. Schlanger, Arnold & Porter LLP

Ronald Lee is a partner and Lauren Schlanger is an associate in Arnold & Porter's Washington, D.C., office.

[1] National Defense Authorization Act of 2013, Pub. L. No. 112-239 (Jan. 2, 2013).

[2] Section 941(e).

[3] Id.

[4] Section 941(c)(1).

[5] Section 941(c)(2).

[6] Section 941(c)(3).

[7] See 76 Fed. Reg. 38089, Safeguarding Unclassified DoD Information (DFARS Case 2011–D039) ((June 29, 2011).

[8] Department of Defense (DOD) — Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, 77 Fed. Reg. 27615 (May 11, 2012). An

advisory discussing this program is available at http://www.arnoldporter.com/public_document.cfm?id=18760&key=11A0.

[9] Joint Statement of the Committee of Conference, available at http://armedservices.house.gov/index.cfm/ndaa-home?p=ndaa.

[10] Id.