WILMERHALE

President Signs New Cybersecurity Provisions in Defense Authorization Act

2013-01-03

On January 2, 2013, President Obama signed the National Defense Authorization Act for Fiscal Year 2013 (NDAA), which includes both new requirements for cleared defense contractors to share information with the Defense Department (DoD) about cyber intrusions and new cybersecurity procurement opportunities.[1]

Reporting and Access Requirements with Respect to Cyber Intrusions

Section 941 of the NDAA gives DoD 90 days to establish procedures requiring "cleared defense contractors"[2] to report to DoD when "covered networks"[3] are successfully penetrated. The procedures must require cleared defense contractors to "rapidly report" to DoD "successful penetration[s]" of covered networks. The reports must describe the technique or method used in the penetration (including a sample of the malicious code, if available) and summarize DoD information that might have been compromised.

The procedures must include mechanisms allowing DoD to access the contractor's system to perform forensic analysis. This access is limited to equipment or information necessary to determine whether and to what extent information created by or for DoD "was successfully exfiltrated . . ." The procedures must protect trade secrets, commercial or financial information, or personally identifiable information. The Act limits DoD's abilities to disseminate information obtained or derived through the procedures outside of DoD, although we note that cleared defense contractors have existing obligations established by the National Industrial Security Program Operating Manual (NISPOM) to report to the FBI and DoD any act of possible of espionage, including certain cyber intrusions.[4] The procedures created to implement Section 941 may require an amendment of the existing NISPOM reporting requirements.

The Joint Statement of the Managers included with the NDAA Conference Report notes that Section 941 is intended to be compatible with the current Defense Federal Acquisition Regulation rulemaking that would mandate cyber breach reporting from an even broader category of contractors.[5] The Statement specifically calls on DoD to consult with industry in developing the

reporting processes and encourages DoD to expand its voluntary Defense Industrial Base information-sharing program.[6]

Under Section 941, DoD will now have 90 days to issue procedures governing the new cyber reporting and access requirements. DoD contractors who may be affected by the procedures should watch this rulemaking closely, and take advantage of any possible DoD solicitation of views on how to implement Section 941. While Section 941does not explicitly require public notice and comment, the complexity of the issue, the limited time frame allotted for DoD to develop the procedures, and the comments in the Managers' Joint Statement urging DoD to consult with industry will likely lead to at least informal engagement with contractors, if not a public comment process.

Cyber Procurement Opportunities

The NDAA also includes various DoD acquisition requirements, which could result in new cyber procurement opportunities. For example, DoD is instructed to develop a strategy to acquire a "next generation system" for cybersecurity tools and capabilities, and must submit a report to Congress with this strategy along with the proposed FY 2015 DoD budget.[7] DoD is also instructed to assess various aspects of DoD's cyber technical capabilities.[8]

---

[1]The full NDAA is available here: http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf. The full Conference Report is here: http://docs.house.gov/billsthisweek/20121217/CRPT-112HRPT-705.pdf. The full Joint Statement of the Managers is available here: http://www.rules.house.gov/Media/file/PDF_112_2/PDF/HR4310crJES.pdf. The cybersecurity title of the NDAA can be found at Title IX: Department of Defense Organization and Management, Subtitle D: Cyberspace-Related Matters. The relevant portions of the Joint Statement of the Managers are on pages 178–189.

[2] "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. Section 941(e)(1).

[3] "Covered networks" are networks or information systems of cleared defense contractors that contain or process information created by or for DOD for which the contractor must apply enhanced protection. Section 941(e)(2).

[4] Defense Security Service, *Industrial Security Letter 2010-02* (Feb. 22, 2010), available at http://www.dss.mil/documents/pressroom/ISL_2010_02.pdf.

[5]The proposed DFARS rule can be found at 75 Fed. Reg. 9563 (Mar. 3, 2010), available at https://www.federalregister.gov/articles/2010/03/03/2010-4173/defense-federal-acquisition-regulation-supplement-safeguarding-unclassified-information-dfars-case.

[6] The current Defense Industrial Base Voluntary Cyber Security and Information Assurance Program was established by an interim final rule in May 2012. 32 CFR 236; 77 Fed. Reg. 27615 (May 11, 2012), available at https://www.federalregister.gov/articles/2012/05/11/2012-10651/department-of-defense-dod-defense-industrial-base-dib-voluntary-cyber-security-and-information. A description of the program can be found here: http://www.acq.osd.mil/dpap/policy/policyvault/OSD012537-12-RES.pdf.

[7] Section 932.

[8] *See, e.g.,* Sections 934 and 936.

Authors

Jamie Gorelick

PARTNER

Chair, Regulatory and Government Affairs Department

jamie.gorelick@wilmerhale.com

+1 202 663 6500

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195