KING & SPALDING

Client Alert

Government Advocacy and Public Policy Group

January 7, 2013

Cybersecurity Provisions Enacted under 2013 National Defense Authorization Act

On January 2, 2013, President Obama signed the 2013 National Defense Authorization Act for 2013 (NDAA) into law.[1] Each year Congress passes the NDAA to authorize funding levels for Department of Defense (DoD) programs and operations and for national security programs in the Department of Energy. In the wake of the failure to enact comprehensive cybersecurity legislation, Congress included several targeted statutory provisions setting federal defense policy on a range of cybersecurity issues.

The NDAA's Cybersecurity Provisions

In recent years, the security of computerized data and the ability of the public and private entities to respond to the unauthorized penetration of computer networks has been intensely debated by policymakers. While concerns over data security have become ubiquitous across industries, the risks associated with data breaches remain a critical concern in the defense industry given the national security information possessed by the Nation's defense industrial base and cleared defense contractor community. In light of the risks to national security, Congress included a series of cybersecurity-related provisions in the NDAA's policy sections—Sections 931 through 941—some of which may impact the defense contracting community, particularly:

- Section 941, which requires the Secretary of Defense to establish mandatory procedures governing reporting requirements on covered defense contractor where a successful cyber-penetration has occurred. The Secretary must promulgate procedures governing mandatory reporting within 90 days of enactment – April 2013;
- Section 935, which authorizes the development and demonstration of collection, processing, and storage technologies for network flow data within DoD and encourages cooperation with the private sector; and
- Section 938, which highlights Congress's concern over potential vulnerabilities in the supply chain.

Mandatory Reporting of Data Breaches

From the perspective of the private sector, the requirement for mandatory reporting by "cleared defense contractors," in Section 941, is perhaps the

For more information, contact:

J.C. Boggs
+1 202 626 2383
jboggs@kslaw.com

Dan Donovan
+1 202 661 7815
ddonovan@kslaw.com

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

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

Tom Spulak
+1 202 661 7948
tspulak@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

most important of these new cybersecurity provisions, and raises the most serious compliance questions. Those questions are heightened given a related pending rulemaking in the Defense Federal Acquisition Regulations (DFAR). Although the Conference Report accompanying the NDAA states that it is Congress's intent that these mandatory reporting requirements "be compatible with, and provide support for, that eventual DFAR rule,"[2] this legislation may, at a minimum, delay the DFAR rule. The NDAA reporting requirements will: (1) apply to all "cleared defense contractors" as defined to mean "a private entity granted clearance [by DoD] to access, received, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of [DoD]," and (2) cover a cleared defense contractor's network or information system containing or processing "information created by or for the [DoD] with respect to which such contractor is required to apply enhanced protection."[3]

Section 941 requires that, within 90 days from enactment, the Secretary of Defense "shall establish procedures that require each cleared defense contractor to report" to the appropriate designated official "when a network or information system of such contractor that meet [the criteria established certain Defense officials] is successfully penetrated." These procedures will require "each cleared defense contractor to rapidly report to [the appropriate designated Defense Department component] each successful penetration" and include in its report: "(A) A description of the technique or method used in such penetration; (B) A sample of the malicious software, if discovered and isolated by the contractor involved in such penetration; [and] (C) A summary of information created by or for the Department in connection with any Department program that has been potentially compromised due to such penetration."[4]

The procedures established by the Secretary must include "mechanisms for [DoD] personnel to, upon request, obtain access to equipment or information of a cleared defense contractor necessary to conduct forensic analysis."[5] The procedures will limit the level of access necessary to that which is required to determine whether information created by or for DoD was "successfully exfiltrated" and, if so, what information was taken. Congress has specified that the 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."[6] The procedures must also prohibit the dissemination of information obtained or derived through the procedural reporting requirements except with the approval of the contractor providing such information.[7]

The associated Conference Report states that Congress expects DoD to consult with industry and build on the existing voluntary information sharing provisions within the defense industrial base. Concerning the scope of reportable information specified in DoD's procedures, the Conference Report states the procedures should generally "exclude access to information that is not essential to understanding and preventing penetrations potentially resulting in the loss of DoD information."[8] Finally, Congress does not intend this reporting provision to apply to "telecommunications and Internet service provider networks that merely transmit DoD information … unless such services are provided under requirements for the enhanced protection."[9]

Collection and Analysis of Network Flow Data

Section 935 authorizes DoD to use existing funding sources and research capabilities "to develop and demonstrate collection, processing, and storage technologies for network flow data" that may be scalable to the volume of Tier 1 Internet Service Providers "to collect and analyze the flow data across their networks," reduce cost, and support three specific capabilities. First, the system must capable of "detect[ing] and identify[ing] cyber security threats, networks of compromised computers, and command and control sites used for managing illicit cyber operations and receiving

information from compromised computers."[10] Second, the system must be capable of "track[ing] illicit cyber operations for attribution of the source."[11] Finally, the system must be capable of "provid[ing] early warning and attack assessment of offensive cyber operations.[12] The Conference Report reveals that the initial purpose of this system is to "improve DOD's capabilities to handle its own voluminous flow data records" with the notion that it could be expanded, voluntarily, to handle data flows through Tier 1 Internet Service Providers.[13] To undertake required research and development, this provision of the NDAA requires that "whenever feasible" the Department of Defense coordinate and cooperate with "Tier 1 Internet Service Providers and other managed security service providers."[14]

Focus on DoD's Supply Chain Including for Contractors and Subcontractors

The NDAA includes a provision expressing the "sense of Congress" concerning risks to DoD networks stemming from vulnerabilities in the supply chain. Congress agrees that DoD "must ensure it maintains full visibility and adequate control of its supply chain, *including subcontractors*, in order to mitigate supply chain exploitation."[15] Congress also acknowledges that the Department of Defense needs authority to mitigate supply chain risks to "information technology systems that fall outside the scope of National Security Systems."[16] The Conference Report expresses Congress's concern that certain private companies "present clear cybersecurity supply chain risks that the U.S. Government must address."[17] Although the NDAA does not create statutory requirements to address these issues, this "sense of Congress" provision suggests the likelihood of future action, by DoD or Congress, in this area..

If you have any questions regarding the NDAA cybersecurity provisions or related issues, please contact Eleanor Hill at +1 202 626 2955 or Alexander Haas at +1 202 626 5502.

---

[1] National Defense Authorization Act for Fiscal Year 2013, Pub. L. 112-___ (Jan. 2, 2013).
[2] H.R. Conf. Rep. 112-705 at 837.
[3] NDAA § 941(e)(1)-(2).
[4] *See id.* § 941(c)(1).
[5] *Id.* § 941(c)(2)(A).
[6] *Id.* § 941(c)(2)(B)-(C)(emphasis added).
[7] *Id.* § 941(c)(3).
[8] H.R. Conf. Rep. 112-705 at 837.
[9] *Id.* at 838.
[10] NDAA § 935(a)(3)(A).
[11] *Id.* § 935(a)(3)(B).
[12] *Id.* § 935(a)(3)(C).
[13] H.R. Conf. Rep. 112-705 at 833.
[14] NDAA § 935(b).
[15] *Id.* § 938(1) (emphasis added).
[16] *Id.* § 938(2).
[17] H.R. Conf. Rep. 112-705 at 835.