Six Recent Government Supply Chain Risk and Cybersecurity Initiatives

August 13, 2018

Key Points

- DoD and other government agencies will scrutinize contractors' supply chain security plans and programs from proposal submission to contract closeout.
- The 2019 NDAA as approved by Congress and DHS initiatives highlight the government's increased focus on supply chain and cybersecurity requirements.

Executive Summary

The Department of Defense (DoD) and other government agencies are continuing to enact initiatives to counter ever-expanding threats to the supply chains of their suppliers of goods and services. These initiatives will increase government contractor compliance requirements and government scrutiny of these compliance programs. We have summarized six of these recent initiatives and what they mean for contractors.

1. DoD to Make Security the Fourth Acquisition Pillar

DoD currently has three pillars in its acquisition framework—cost, schedule and performance. DoD would make security the fourth pillar in defense acquisition in order to "create incentives for industry to embrace security, not as a cost burden, but as a major factor in their competitiveness for U.S. government business," according to Deputy Under Secretary of Defense for Intelligence Kari Bingen.

The pilot program "Deliver Uncompromised" is part of DoD's plan to establish security as the fourth acquisition pillar. According to DoD Joint Testimony on June 21, 2018, the "Deliver Uncompromised" initiative is "focused on industry delivery of capabilities, services, technologies, and weapons systems that are uncompromised by our adversaries from cradle-to-grave." This will likely entail establishment of cybersecurity and other supply chain security as a significant evaluation factor.

Contact

Robert K. Huffman
rhuffman@akingump.com
Washington, D.C.
+1 202.887.4530

Natasha G. Kohne
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
mreed@akingump.com
Dallas
+1 214.969.2713

Joseph W. Whitehead
jwhitehead@akingump.com
Washington, D.C.
+1 202.887.4477

Chris Chamberlain
cchamberlain@akingump.com
Washington, D.C.
+1 202.887.4308

Amanda B. Lowe
alowe@akingump.com
Washington, D.C.
+1 202.887.4461

2. Combatting Supply Chain Risk (Section 881 NDAA)

Section 881 of the 2019 NDAA as approved by Congress bolsters the federal government's ability to combat supply chain risk[1] by empowering the Secretary of Defense and the Secretaries of the Army, Navy and Air Force to exclude contractors from certain procurement actions in the interest of national security and to limit the disclosure of information relating to these exclusions. While the DFARS already includes a "Supply Chain Risk" Clause, 252.239-7018 (Oct. 2015), the Section 881 authority does not depend upon the presence of an implementing clause in the solicitation or contract, and it could serve as authority for DoD's "Do Not Buy" Software List discussed in Section 4 below.

Under Section 881, if an agency head determines that a significant supply chain risk exists in the procurement of a national security system[2] or an item of information technology purchased for inclusion in a national security system, it may (1) exclude from the procurement "a source that fails to meet qualification standards established… for the purpose of reducing supply chain risk"; (2) "[exclude] a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a delivery order"; or (3) "[decide] to withhold consent for a contractor to subcontract with a particular source or to direct a contractor for a covered system to exclude a particular source from consideration for a subcontract."

If the agency head also exercises the authority to limit disclosure of information, "no action undertaken by the agency head under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court." The agency head must "notify appropriate parties of a covered procurement action and the basis for such action," but "only to the extent necessary to effectuate the covered procurement action." Moreover, the agency head must "notify other Department of Defense components or other Federal agencies responsible for procurements that may be subject to the same or similar supply chain risk."

To exercise these authorities under Section 881, the agency head must obtain a joint recommendation from the "Under Secretary of Defense for Acquisition and Sustainment and the [DOD] Chief Information Officer, on the basis of a risk assessment by the Under Secretary of Defense for Intelligence, that there is a significant supply chain risk." The agency head must also determine in writing that (1) the use of the authority is necessary to protect national security; (2) "less intrusive measures are not reasonably available"; and (3) if disclosure will be limited, "the risk to national security due to the disclosure of such information outweighs the risk due to not disclosing such information." Finally, a classified or unclassified notice of this determination must be made to the "appropriate congressional committees," which include the Permanent Select Committee on Intelligence of the House of Representatives, as well as all of the congressional defense committees.

Section 881 is a powerful tool for federal enforcement of supply chain risk management, and, in some cases, it virtually eliminates the ability of contractors to protest these procurement decisions or to learn the basis for such decisions. As a result, contractors and subcontractors participating in procurements for national security systems will likely need to take additional steps to strengthen their own supply chain vetting as part of the procurement process, or risk being excluded from DoD and other federal procurement actions for reasons that may never be fully explained.

3. Strengthening Cybersecurity Requirements (NDAA Subtitle C)

The 2019 NDAA as approved by Congress also focuses extensively on improving and strengthening cybersecurity requirements in DoD, from structural reforms to vulnerability assessments and cooperation with the civilian sector. The NDAA devotes an entire subsection (Sections 1631-1657) to cybersecurity. Among these numerous provisions in the NDAA, Section 1636 announces that it is the policy of the United States to "employ all instruments of national power, including the use of offensive cyber capabilities," to deter and respond to cyber-attacks or malicious cyber activities of foreign powers. Section 1642 specifically authorizes DoD to respond to cyber activities conducted against the United States by Russia, China, North Korea and Iran, and permits DoD to cooperate with the private sector in sharing threat information on a voluntary basis. To better prepare for hostile, foreign cyber activities, Section 1649 requires DoD to "carry out a pilot program to model cyber-attacks on critical infrastructure in order to identify and develop means of improving Department of Defense responses to requests for defense support to civil authorities for such attacks."

In addition, Section 1644 directs DoD to "enhance awareness of cybersecurity threats among small manufacturers and universities working on Department of Defense programs and activities." This program will involve several aspects, including outreach; education; transfer of technology, threat information and techniques; and a cyber counseling certification program to "certify small business professionals and other relevant acquisition staff within the Department of Defense to provide cyber planning assistance to small manufacturers and universities."

The heavy focus on cybersecurity in the 2019 NDAA as approved by Congress demonstrates its continuing importance in national defense and security. As a result, government contractors should be prepared for increased government focus on cyber issues in procurement and operations.

4. DoD Confirms Existence of "Do Not Buy" Software List

On July 27, 2018, the DoD Undersecretary for Acquisition and Sustainment, Ellen Lord, confirmed the existence of a "Do Not Buy" list of software that does not meet "national security standards." While the list is not available, reports indicate that it generally includes software that is of Russian and Chinese origin or that does not meet certain defense standards. In addition to the technical intelligence, defense and security issues related to this list, it may also cause problems for contractors responding to DoD solicitations that include software requirements.

Because this list is not available, contractors will not know if their proposed software solution is acceptable. This issue is exacerbated by contractors relying on subcontractors, vendors and teaming partners to provide software solutions. Indeed, Ms. Lord reportedly stated that even the DoD has trouble determining the provenance of software due to complicated supply chains and holding companies.

DoD may encounter certain legal and regulatory hurdles by maintaining this undisclosed and informal list. For example, if an offeror's proposal is disqualified because its software solution is on the "Do Not Buy" list, a protest could be sustained

because DoD used unstated evaluation criteria. *These issues may be mitigated by Section 881 of the NDAA as discussed above*.

We will continue to monitor this issue and the related legal issues for government contractors.

5. Government Agencies are Conducting Cybersecurity Reviews

We have heard that contractors are receiving cybersecurity review notices from certain agencies, including the Navy and the Missile Defense Agency. We understand that these reviews may be going beyond the NIST SP 800-171 requirements and are also focusing on contractors' internal training. This action shows that agencies are moving beyond the evaluation of contractors' system security plans (SSP). Contractors should be prepared to demonstrate to the agency that they are actually implementing what is in their SSPs. Contractors should also consider whether, and how, to push against agencies' attempts to review cybersecurity issues beyond the scope of the NIST 800-171 requirements.

6. DHS Announces National Risk Management Center

On July 31, 2018, Department of Homeland Security (DHS) Secretary Kirstjen Nielsen unveiled the DHS's new National Risk Management Center (NRMC) at a cybersecurity summit in New York. Secretary Nielsen highlighted the new division's focus on fostering public-private collaboration in U.S. critical infrastructure protection. NRMC will be directed by Bob Kolasky, currently Acting Assistant Secretary of Infrastructure protection at DHS's National Protection and Programs Directorate.

Initial program guidance (See DHS NRMC fact sheet) outlines NRMC's key functions and "immediate actions," including:

- identifying, assessing and prioritizing risks to national critical functions, including by developing risk registries and dependency analyses "with a focus on lifeline functions"
- collaborating on the development of risk management strategies and approaches to manage risks to national critical functions, including development of a strategic framework to identify critical, cross-sector cyber supply supply-chain elements
- coordinating integrated cross-sector risk management activities, including establishing a "cross-sector, government/industry playbook" for executing integrated risk management activities.

One key purpose of the new NRMC is to separate strategic planning and private-sector, information-sharing functions from the core "real-time" functions of DHS's existing National Cybersecurity and Communications Integration Center (NCCIC) (e.g., incident response and threat indicator sharing). DHS established NCCIC in 2009 as a threat-monitoring hub, but its focus has since shifted to include private-sector collaboration, particularly in the wake of the Cybersecurity Information Sharing Act (CISA) of 2015. Practically speaking, a key impetus for DHS's NRMC is the industry's lagging participation in threat information sharing, which, notwithstanding CISA's

liability limitations, has been undermined by industry concerns that sharing information will increase the risk of regulatory and cybersecurity vulnerability exposure.

Another key concern going forward for companies with both DoD and DHS contracts will be consistency between DoD cybersecurity requirements (i.e., DFARS Clause - 7012 and NIST SP 800-171) and DHS's information-sharing and strategic-planning efforts. Broadly speaking, the NRMC is closely related to the NIST Cybersecurity Framework and NIST's Cyber Supply Chain Risk Management (C-SCRM) Program, among other cybersecurity and critical infrastructure initiatives flowing from Executive Order 13636 and Presidential Policy Directive (PPD)-21. For that reason, in the absence of more specific guidance from DHS, organizations familiar with related NIST standards and controls will likely find synergies by integrating supply chain risk management and collaboration into existing security operations and planning (e.g., as part of developing System Security Plans and implementing specific supply-chain related and monitoring controls) (e.g., SP 800-171 controls 3.1.20, 3.2.2, 3.6.1 and 3.14.3, among others). Separately, NIST publishes detailed guidance (in Special Publication 800-161) and case studies on supply chain risk management that companies should consult in developing and executing risk management plans and strategic planning.

---

[1] The Act defines "supply chain risk" as "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."

[2] "National security system" is defined in 44 U.S.C. § 3542(b)(2)(A) as "any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which: (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) … is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized… to be kept classified in the interest of national defense or foreign policy." This definition does not include "a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications)."