COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Government Contracts

January 9, 2014

NEW INTELLIGENCE COMMUNITY DIRECTIVE ADDRESSES SUPPLY CHAIN RISK MANAGEMENT

On December 7, 2013, the Director of National Intelligence ("DNI") issued Intelligence Community ("IC") Directive 731 ("the Directive"). The Directive represents another step in a continuing trend by the Government to protect supply chain integrity, as it follows several recent proposed, interim, and final rules issued by the Department of Defense ("DoD").

BACKGROUND

The purpose of the Directive is to establish IC policies to protect the integrity and authenticity of "mission-critical products, materials, and services" within the supply chains utilized by IC elements. The term "mission-critical products, materials, and services" is not defined in the Directive or any other publicly-available IC directives; however, based on the description of "criticality assessments" within the Directive and a similar term defined in DoD Instruction 5200.44,[1] the term likely refers to a product, material, or service, the compromise of which would harm an organization's operation or core mission.

To achieve its stated purpose, the Directive establishes a procedure for the identification, assessment, and mitigation of supply chain threats through the use of comprehensive risk assessments, the establishment and maintenance of a "common collaborative environment" within the IC for sharing supply chain threat information and risk management best practices ("the Forum"), and regular training in relevant counterintelligence, security, acquisition, and civil liberties principles and practices for all IC personnel involved in supply chain management.

The policies outlined by the Directive apply to procurements of all mission-critical products, materials, and services at all stages of the acquisition process, from requirements development through decommissioning or retirement.

RISK ASSESSMENTS

The Directive's primary and most significant method for protecting IC supply chains is the implementation of risk assessments. The Directive requires that IC elements conduct risk assessments (1) "for the acquisition of products, materials, and services deemed mission-critical by the heads of IC elements," and (2) "for all IC products, materials, and services where the DNI has determined the risk warrants a standard approach to the mitigation."

[1] DoDI 5200.44 (Nov. 2012) defines "mission-critical function" as "any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed."

Risk assessments consist of four items:

1. a threat assessment of the proposed contractor, subcontractor, vendor, and/or verified sub-vendor;
2. a vulnerability assessment of the proposed acquisition;
3. an assessment of the potential harm to the IC element's operations or mission caused by the possible loss, damage, or compromise of the products, materials, and/or services being procured (a "criticality assessment"); and
4. applicable mitigation information.

IC elements are required to complete risk assessments as early in the acquisition process as possible and to mitigate risk throughout the acquisition process. The Directive requires completed risk assessments and any associated mitigation plans to be reviewed every two years to determine if modifications are necessary due to changed conditions within the supply chain.

The results of threat assessments will be produced and shared within the newly-created Forum, and the vulnerability and mitigation information will be discoverable within the Forum consistent with IC Directive 501, Discovery and Dissemination or Retrieval of Information within the Intelligence Community. It is unclear as to whether the criticality assessments are discoverable or meant to be shared within the IC.

The Directive specifically permits the exclusion of contractors, subcontractors, or vendors from procurements of information technology ("IT") based on supply chain risk factors identified during the risk assessment. This exclusion is based on DNI's authority under 50 U.S.C. § 3329, note.[2] If a contractor is excluded due to supply chain risk, the public disclosure of that exclusion may be limited when necessary to protect national security. As a result, a contractor may not understand the basis for its exclusion, nor would the basis likely be discoverable in a subsequent bid protest. Just as with DoD's version of this rule (discussed below), this exclusion right raises the prospect of defacto debarments of contractors as this decision is shared within the Forum. Although there may be no public disclosure, a decision to exclude a contractor must be reported to the relevant congressional intelligence committee and must summarize the basis for the determination, including an explanation for why a less intrusive solution is not reasonably available.

This is similar to the authority granted to DoD in Section 806 of the National Defense Authorization Act ("NDAA") of FY 11 and to the Department of Energy in section 3113 of the recently passed FY 14 NDAA. As discussed below, DoD promulgated an interim rule implementing Section 806 in November 2013. Interestingly, in the Explanatory Statement that accompanies the FY 14 NDAA, Congress indicated that it expected DOE to use its exclusion authority on only an infrequent basis and encouraged DOE to partner with supply chain sources to the extent possible.

---

2 Section 309 of the Intelligence Authorization Act of 2012, provided DNI with enhanced procurement authority to manage supply chain risks. *See* 50 U.S.C. § 3329, note. Pursuant to this authority, the head of an IC element (other than within DoD), in consultation with DNI, may, with regard to IT contracts: (1) exclude a source that fails to meet qualifications standards established in accordance with the requirements of 41 U.S.C. § 3311, for the purpose of reducing supply chain risk in the acquisition of covered systems; (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 task or delivery order; and/or (3) 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 under the contract.

IMPACT ON CONTRACTORS AND RELATION TO OTHER RECENT SUPPLY CHAIN RULES

Although the Directive is an internal IC policy and imposes no direct responsibilities on contractors, it provides further evidence of the Government's increasing concerns with vulnerabilities within its supply chain. As the Directive notes, supply chain risk is inherent in "supply chains that interface with or operate in a global marketplace." Moreover, some aspects of this Directive are consistent with other recent supply chain regulations issued by DoD.

On November 18, 2013, DoD issued an interim rule for supply chain risk management, which implements Section 806 of the FY 11 NDAA. Similar to the authority granted to the IC, DoD may exclude certain information technology ("IT") contractors from procurements if a DoD risk assessment demonstrates that the IT contractor fails to meet qualification standards necessary for reducing supply chain risk in the acquisition of IT for National Security Systems. As a result, IT contractors contracting with the IC or DoD should consider taking proactive measures in response to the Directive and DoD interim rule by reviewing and strengthening their supply chain security and evaluating their subcontractors' supply chain risks.

Additionally, DoD issued a final rule on December 16, 2013 to strengthen supply chain integrity by revising requirements for contractors to use unique markings and identify the cost of items delivered under DoD contracts. The rule requires the use of item unique identification ("IUID") when the Government's acquisition cost for an item is at least $5,000 or where the item is mission-essential or serially managed. The final rule clarifies that expenses associated with implementing the item unique identifiers will be recognized as allowable costs, but makes no provision for the recovery of these costs separately in a fixed price environment.

Finally, DoD issued a proposed rule on May 16, 2013 for the detection and avoidance of counterfeit electronic parts. The proposed rule required contractors to establish a counterfeit electronic parts avoidance and detection system. The Directive is broader than the proposed rule, as the proposed rule applies only to counterfeit *electronic* parts, and the Directive applies to *all* products and materials in the IC supply chain. In lieu of the Directive, and given that DoD is expected to issue a final rule in Spring 2014, contractors should review their procedures for detecting and preventing the use of counterfeit parts.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our government contracts practice group:

David Fagan	202.662.5291	dfagan@cov.com
Susan Cassidy	202.662.5348	scassidy@cov.com
James Garland	202.662.5337	jgarland@cov.com
Roger Zakheim	202.662.5959	rzakheim@cov.com
Catlin Meade	202.662.5889	cmeade@cov.com