NEW DFARS RULES ADDRESS SUPPLY CHAIN RISKS AND UNCLASSIFIED INFORMATION

This client alert provides an update on two notable recent security and information assurance-related rules promulgated by the Department of Defense ("DoD") amending the Defense Federal Acquisition Regulation Supplement ("DFARS"): (1) an interim rule implementing legislatively mandated requirements to address supply chain risk to allow DoD to consider the impact of "supply chain risks" in information technology ("IT") contracts; and (2) a final rule on the safeguarding of unclassified controlled technical information ("UCTI"), which includes, among other things, certain cyber incident reporting obligations. These two rules are described further below.

INTERIM DFARS RULE REQUIRES EVALUATION OF SUPPLY CHAIN RISKS IN CERTAIN IT CONTRACTS

On November 18, 2013, DoD issued an interim rule amending the DFARS to allow DoD to consider the impact of "supply chain risks" in information technology ("IT") contracts. The interim rule creates new solicitation and contract clauses that apply to all solicitations and contracts involving the development or delivery of any IT, including contracts for commercial items or commercial off-the-shelf items. The contract clause must be included in all subcontracts involving the development or delivery of any information technology, either as a service or a supply, and contracting officers are encouraged to consider a Government consent requirement in the prime contract for all such subcontracts.

The DFARS interim rule is significant because it provides DoD with authority to exclude IT contractors from contract participation and withhold consent for contractors to use certain subcontractors if the Department determines that a contractor or subcontractor presents a supply chain risk (a "Section 806 Action").

Background

The DFARS interim rule implements Section 806 of the National Defense Authorization Act ("NDAA") for Fiscal Year 2011, Pub. L. No. 111–383, as amended by the NDAA for Fiscal Year 2013, Pub. L. No. 112–239, entitled “Requirements for Information Relating to Supply Chain Risk.” The interim rule is in response to Congress’ growing concern about DoD’s supply chain risks. The Senate first took action on this issue in 2010 by including language in the NDAA for Fiscal Year 2011 that authorized the head of a defense agency to address supply chain risk in the acquisition of national security systems. The NDAA for Fiscal Year 2011 conference agreement adopted the Senate language and clarified the circumstances in which the head of a defense agency could take actions to address supply chain risk. The NDAA for Fiscal Year 2013 extended Section 806 to September 30, 2018, as well as required DoD to assess the effectiveness of Section 806 and report the results to Congress.
Three years after the initial enactment, the interim final rule marks an important step in the implementation of Section 806.

Key Definitions

Under the NDAA, Section 806 Actions are permitted in procurements for “information technology” for a “covered system,” where there is a “supply chain risk.” The interim rule defines these key terms as follows:

- **“Information technology”:** In lieu of the definition at FAR 2.1, any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

- **“Covered system”:** A National Security System (“NSS”), see 44 U.S.C. § 3542(b)(2)(A), which means 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:
  1. 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, but does not include a system that is to be used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications; or
  2. Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

- **“Supply chain risk”:** 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.

Section 806 Actions

The interim rule authorizes DoD to employ three different supply-chain risk management actions with respect to DoD solicitations for covered systems:

1. Exclude a source that fails to meet qualification standards 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
3. Withhold consent for a contractor to subcontract with a particular source or direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract.
In addition, DoD can limit disclosure of information relating to its Section 806 Actions. In such instances, the Section 806 Action will not be reviewable in a bid protest before the Government Accountability Office (“GAO”) or any federal court.

Although the interim rule dictates that the accompanying clause be included in all IT solicitations and contracts, Section 806 Actions are limited to procurements of NSS or “covered items of supply.” A covered item of supply is an IT item purchased for inclusion in an NSS, the “loss of integrity of which could result in a supply chain risk.”

The responsibility for making a Section 806 Action is limited to “authorized individuals,” who include the Secretaries of Defense, the Army, the Navy, and the Air Force; the Under Secretary of Defense for Acquisition, Technology, and Logistics; and, for military departments, the senior acquisition executive for each department. Section 806 Actions require three steps: recommendation, determination, and notification. Authorized officials must obtain a joint recommendation from the Under Secretary of Defense for Acquisition, Technology, and Logistics and the DoD Chief Information Officer, based on a risk assessment by the Under Secretary of Defense for Intelligence, that there is a significant supply chain risk to a covered system. Authorized officials must then make a written determination that the Section 806 Action is (1) necessary to protect national security by reducing a supply chain risk, (2) less intrusive measures to reduce the security risk are not reasonably available, and (3) if the official plans to limit disclosure of information, that the risk to national security from disclosure outweighs the risk of not disclosing such information. Finally, authorized officials must provide written notice of a Section 806 Action to congressional defense and intelligence committees and to other DoD components or federal agencies responsible for procurement that may carry the same or similar supply chain risks.

Impact on Contractors

The DFARS interim rule outlined above could have a considerable impact on IT contractors working with DoD. The rule’s introduction of Section 806 Actions carries serious consequences—namely, exclusion—for contractors with inadequate supply chain security. Even if a contractor initially qualifies for an award, failure to comply with the clause’s requirements to “maintain controls in the provision of supplies and services to the Government to minimize supply chain risk” could result in a contract breach and all the adverse consequences that result from such a breach.

The rule neither delineates policies or procedures nor mandates any specific reporting, recordkeeping, or other requirements for complying with the Section 806 program. It does, however, “recognize the need for information technology contractors to implement appropriate safeguards and countermeasures to minimize supply chain risk.” It is left to “the individual contractors to take the steps they think are necessary to maintain existing or otherwise required safeguards and countermeasures as necessary for their own particular industrial methods to protect their supply chain.”

Section 806 includes a “sunset” provision, which provides that its authority expires on September 30, 2018. DoD must report to Congress on the effectiveness of this authority by January 1, 2017. Public comments on the interim rule must be submitted on or before January 17, 2014.

**DFARS Final Rule Implements Measures to Safeguard DoD UCTI**

On November 18, 2013, DoD issued a final rule on the safeguarding of unclassified controlled technical information (“UCTI”), which imposes requirements for (1) safeguarding UCTI that is “resident on or transiting through contractor unclassified information systems,” and (2) reporting...
cyber incidents and UCTI compromises. Controlled technical information is “technical information with military or space application . . . subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.” Information that is “lawfully publicly available” does not qualify as UCTI.

The final rule adds a new subpart and a corresponding contract clause to the DFARS requiring DoD and its contractors to provide “adequate security” to safeguard UCTI on unclassified information systems. Although the new clause must be included in all solicitations and contracts, including solicitations and contracts for the acquisition of commercial items, the safeguarding measures will only apply when UCTI is present. Contractors must flow down the substance of the clause to all subcontractors.

To provide adequate security, the contract clause created by the final rule requires a contractor to either (1) implement an information system security program that, at a minimum, includes specified security controls from National Institute of Standards and Technology (“NIST”) Special Publication (“SP”) 800-53, or (2) provide the contracting officer with a written explanation that either explains why such controls are not required or specifies alternative controls or protective measures that achieve the same level of protection. There are 51 required NIST controls, each of which are listed in Table 1 of the rule. Contractors are also obligated to apply any other security measures that the contractor reasonably determines is necessary to provide adequate security.

The final rule also imposes requirements for reporting cyber incidents and assisting DoD with damage assessments. Contractors are obligated to report specified information to DoD via http://dibnet.dod.mil/ within 72 hours of discovery of any cyber incident. Types of reportable cyber incidents include unauthorized access to information, inadvertent release of information, and/or any other loss or compromise. Following a cyber incident, contractors also are required to provide support to DoD damage assessments. In particular, contractors are required to (1) conduct further reviews of their networks “to identify compromised computers, servers, specific data and users accounts,” (2) review the data accessed during the cyber incident to identify specific UCTI associated with DoD programs, systems, or contracts, and (3) preserve and protect images of known affected information systems and all relevant capture data for at least ninety (90) days to allow DoD to request information or decline interest.

Impact on Contractors

The final rule provides no guidance on how compliance with the requirements of the clause will be judged but potentially imposes significant requirements on contractors’ information systems. Contractors that fail to meet the requirements in the clause could be in breach of their contract, with all the adverse consequences that result from such a breach. Although not addressed directly in the proposed DFARS clause, DoD’s responses to comments on the proposed rule clarified that while the Government will not “directly pay for the operating costs associated with the rule,” costs associated with implementation will be allowable and chargeable to indirect cost pools. This could present a challenge to commercial and other contractors that operate on a fixed priced basis with the Government.
If you have any questions concerning the material discussed in this client alert, please contact the following members of our firm:

Susan Cassidy +1.202.662.5348 scassidy@cov.com
David Fagan +1.202.662.5291 dfagan@cov.com
Alan Pemberton +1.202.662.5642 apemberton@cov.com
Jennifer Plitsch +1.202.662.5611 jplitsch@cov.com
Roger Zakheim +1.202.662.5959 rzakheim@cov.com
Peter Colwell +1.202.662.5587 pcolwell@cov.com
Catlin Meade +1.202.662.5889 cmeade@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.

© 2013 Covington & Burling LLP, 1201 Pennsylvania Avenue, NW, Washington, DC 20004-2401. All rights reserved.