Published by *Government Contracts Law360* on December 4, 2013. Also ran in *Aerospace & Defense Law360, Privacy Law360*, *Public Policy Law 360*, and *Technology Law360*.

Thoughts On DOD Rules For Cybersecurity, Supply Chain Risk

--By Ronald D. Lee, Nicholas L. Townsend and Lauren J. Schlanger, Arnold & Porter LLP

Law360, New York (December 04, 2013, 1:13 PM ET) -- On Nov. 18, 2013, the U.S. Department of Defense published two rules[1] that impose new cybersecurity requirements on its contractors and subcontractors and address supply chain risk. Given the dim prospects for enactment of comprehensive cybersecurity legislation in the current political environment on Capitol Hill, these rules are an important part of the Obama administration's efforts to use the government's procurement power and existing regulatory authorities to increase the cybersecurity of the companies on which the U.S. government relies.

First, the DOD published a final rule that will require contractors and subcontractors to: (1) report "cyber incidents" that affect unclassified controlled technical information (UCTI), and (2) provide "adequate security" to safeguard UCTI from compromise. These new cybersecurity requirements will be incorporated into all DOD solicitations and contracts and will apply to a broad variety of private sector information systems that contain DOD UCTI, although the final rule is somewhat narrower in scope than the proposed rule the DOD published in June 2011.

Second, the DOD published an interim rule that would allow the secretary of defense and the secretaries of the military departments to exclude from any covered procurement related to a national security system a source that fails to meet supply chain risk qualification standards or fails to achieve an acceptable rating for supply chain risk. Under the rule, which implements the authority first set out in Section 806 of the National Defense Authorization Act for Fiscal Year 2011, the DOD would also be able to direct a contractor to exclude a particular source from consideration for a subcontract or withhold consent for a contractor to subcontract with a particular source.

The interim rule adds a new solicitation provision and contract clause to be included in future IT procurements notifying contractors of the government's right to exercise this authority. The interim rule requires contractors to "maintain controls in the provision of supplies and services to the Government to minimize supply chain risk" and places contractors on notice of a general obligation to manage supply chain risk and the actions the DOD may take to safeguard the supply chain.

Final DOD Cyber Rule on UCTI

Cyber Incident Reporting

DOD contractors and subcontractors who have UCTI resident on or transiting through their information systems will be required to file a report with the DOD within 72 hours of discovering a cyber incident that affects UCTI. A "cyber incident" means "actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein."

This would include an incident involving possible exfiltration, manipulation or other loss or compromise of any UCTI resident on or transiting through a contractor's unclassified information systems or any other activities that allow unauthorized access to such information systems.

This broad definition of cyber incident could potentially include both advanced cyber attacks and low-tech occurrences, such as an employee with access to UCTI writing his computer password on a post-it note that is visible to unauthorized persons.

The DOD's final rule reduces the scope of this reporting requirement (as well as the safeguarding requirement discussed below) as compared to the interim rule the DOD published in June 2011 by limiting the information covered to only UCTI. UCTI includes "technical information with military or space application that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination."

Cyber incident reports must disclose 13 items, including type, date and location of the compromise, the technical information and DOD programs, platforms or systems involved, and basic information regarding the contractor. Such reports must be filed online.

In addition to reporting the incident, contractors and subcontractors are required to (1) conduct further review for evidence of compromise resulting from the cyber incident; (2) review the data accessed during the incident to identify specific UCTI associated with DOD programs, systems or contracts; and (3) preserve and protect images of known affected information systems and relevant monitoring/packet capture data for at least 90 days from the cyber incident.

If the DOD decides to conduct a damage assessment, the contractor must provide the DOD with all the information listed above. This includes sharing files and images, unless there are legal restrictions that limit the contractor's ability to share digital media.

These requirements raise a number of potential issues for government contractors, in addition to the increased cost associated with their implementation. For example, information contained in a contractor's cyber incident report may be protected by nondisclosure agreements or legal restrictions, creating a risk that the contractor could be liable to a third-party for disclosing the information to the government. It is also possible that the contractor and the DOD's contracting officer may disagree on whether the contractor's legal obligations preclude it from turning information over to the DOD. If they are unable to resolve their disagreement, the DOD may take the position that the contractor has breached the contract clause.

Given that the final rule lists "facilitat[ing] information sharing and collaboration and standardiz[ing] procedures for tracking and reporting compromise of information" as among the purposes of the final rule, there is also a risk that the DOD may share threat information derived from incident reports with other private sector companies, which could theoretically result in a contractor's own proprietary data or trade secrets being disclosed to competitors.

For example, information derived from cyber incident reports might be shared as part of the Defense Industrial Base (DIB) Cyber Security and Information Assurance (CS/IA) Program, which the final rule describes as "mutually supportive" with the rule's new cybersecurity requirements.

The DOD's rule governing the DIB CS/IA Program requires that the government take "reasonable steps to protect against the unauthorized use or release" of certain attribution information and other nonpublic information received from a DIB CS/IA participant or derived from such information. By contrast, the DOD's final rule on reporting of cyber incidents involving UCTI merely requires the DOD to protect information reported in cyber incident reports "in accordance with applicable statutes, regulations, and policies" and it limits government disclosure of such information "to authorized persons for purposes and activities consistent with this clause." However, it does not define "authorized person" nor does it specify what activities would be deemed "consistent."

Moreover, negative information in a cyber incident report could harm the ability of the contractor who filed the report to win future government contracts if the DOD concludes that the contractor has inadequate information security procedures that pose a cybersecurity risk. The final rule does not provide a "safe harbor" for companies that file cyber incident reports.

It provides that "a cyber incident that is properly reported by the contractor shall not, by itself, be interpreted under this clause as evidence that the contractor has failed to provide adequate information safeguards for unclassified controlled technical information, or has otherwise failed to meet the requirements of the clause at 252.204-7012." However, the rule also requires the contracting officer to "consider such cyber incidents in the context of an overall assessment of the contractor's compliance with the requirements" of the clause.

Prime contractors must also bear the administrative burden of ensuring subcontractor compliance. Prime contractors are responsible for incorporating these new requirements into their subcontracts at all tiers. Importantly, the final rule does not exclude small businesses that have UCTI from either the safeguarding or the cyber incident reporting requirements.

The rule also requires that the prime contractor report all incidents where UCTI has potentially been compromised "regardless of whether the incident occurred on a prime contractor's information system or on a subcontractor's information system." This may be particularly burdensome given the volume of cyber incident reports that will likely be required under the rule.

The DOD suggests that five reports per company per year will be required with an average of 3.5 hours to prepare each report, which is a substantial increase over the estimate in the DOD's 2011 interim rule due to the relatively high volume of reports that have been made under the DIB CS/IA Program. Some have suggested that the numbers are likely to be much higher. Aside from the cost to prime contractors of submitting such reports, subcontractors may be required to provide cyber incident details, including information system details, trade secrets or other proprietary information to the prime contractor in order to file a complete report.

Safeguarding Requirements

Under the new contract clause published in the final rule, DOD contractors and subcontractors will also be required to provide "adequate security" to safeguard UCTI from compromise. "Adequate security" is defined as "protective measures that are commensurate with the consequences and

probability of loss, misuse, or unauthorized access to, or modification of information." This definition is predictive and harm-based, but contractors or subcontractors likely will not always be in a position to make accurate assessments of the extent of harm to the DOD of compromise of particular UCTI.

In order to provide "adequate security," contractors and subcontractors must implement information systems security in their project, enterprise, or company-wide unclassified IT systems that have UCTI resident on or transiting through them. At a minimum, such information systems security program must implement certain security controls under National Institute of Standards and Technology Special Publication 800-53. The required NIST controls include, among others, standards for authentication, training, incident response, contingency planning, and access controls. If these NIST security controls are not implemented, the contractor must submit a written explanation to the contracting officer.

Given that many contractors likely do not have separate networks for UCTI or a mechanism for separating UCTI from other information on their corporate networks, the DOD's new safeguarding requirements are likely to apply to a large number of contractor IT systems. In the case of large defense contractors, the new safeguarding provisions may not require extensive changes because NIST Special Publication 800-53 closely parallels the ISO 27002 standard, so many big companies are likely already following these industry best practices.

However, small businesses, including many subcontractors, often have less sophisticated IT capabilities. As noted above, the final rule does not exclude small businesses with UCTI from its safeguarding or cyber incident reporting requirements. Smaller companies may need to incur significant costs in order to meet the new UCTI safeguarding requirements and establish an adequate information systems security program. However, the final rule explicitly states that "the contractor's size classification is not a sufficient reason to allow a contractor to fail to protect technical information."

The DOD's final rule suggests that the costs associated with compliance with these Defense Federal Acquisition Regulation Supplement changes may be allowable under the Cost Accounting Standards set out in FAR 31.201-2, but the rule states that the government "does not intend to directly pay for the operating costs associated with the rule." In addition, as noted above, subcontractors are required to have mechanisms to identify and report covered "cyber incidents" to the prime contractor.

Interim Rule on Supply Chain Risk

The interim DFARS rule on supply chain risk implements the authority set forth in Section 806 of the NDAA for FY 2011 (Pub. L. 111–383), titled "Requirements for Information Relating to Supply Chain Risk," and amended by section 806 of the NDAA for FY 2013 (Pub. L. 112–239). Those provisions authorize the DOD to consider the impact of supply chain risk in specified types of IT procurements related to national security systems and take certain actions to manage supply chain risk.

"Supply chain risk" is defined 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 national security system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."

Under Section 806, the DOD is authorized, when conducting a "covered procurement," to:

- exclude a source that fails to meet qualification standards for the purpose of reducing supply chain risk in the acquisition of covered systems;
- 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; or
- withhold consent for a contractor to subcontract with a particular source or direct a contractor to exclude a particular source from consideration for a subcontract.

When exercising Section 806 authority, the DOD may limit disclosure of information relating to the basis for the exclusion, and may notify other federal agencies responsible for procurements that may face similar supply chain risk. The new DFARS interim rule implements and clarifies the DOD's authority to limit disclosure of information relating to the basis for a Section 806 exclusion action. Under the new rule, if the DOD limits disclosure of information, "no action" undertaken by an authorized individual "shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court."

The new rule further provides that when the DOD limits disclosure of information relating to a Section 806 action, notifications to unsuccessful offerors and post-award debriefings may not reveal any withheld information. Accordingly, it is possible that contractors subject to a Section 806 exclusion may not receive notice of the basis for the exclusion and may have no recourse to challenge such exclusion.

The new DFARS interim rule requires inclusion of new solicitation provision and supply chain risk contract clause in all solicitations, including FAR Part 12 commercial item acquisitions, "that involve the development or delivery of any information technology whether acquired as a service or a supply." The new contract clause advises contractors of the government's right to exercise its Section 806 exclusion authority. Although the interim rule does not impose particular procedures or requirements on contractors to manage supply chain risk, the new contract clause instructs that a contractor "shall maintain controls in the provision of supplies and services to the Government to minimize supply chain risk." A failure to manage supply chain risk, therefore, may constitute breach of contract.

Further, the new rule directs that the DOD should consider in all IT solicitations whether there is a need for a consent to subcontract requirement regarding supply chain risk. Overall, under these new rules, the DOD has broad authority to manage supply chain risk through exclusion of sources that threaten national security systems, and may consider risk at all tiers. Prime contractors may be required to forego some autonomy in selecting subcontractors to prevent threats to the supply.

While Section 806 affords the DOD significant authority to manage supply chain risk, by its terms, Section 806 limits the applicability of the DOD's authority to exclude a source. The DFARS interim rule implements several key limiting provisions that restrain use of Section 806 exclusion authority.

Foremost, exercise of Section 806 exclusion authority is limited to "covered procurements," defined as procurements of information technology items for use in national security systems and "the loss of integrity of which could result in a supply chain risk" for the covered system.

A national security system is an information system, including a telecommunications system, that is used for intelligence activities or cryptologic activities related to national security; for command and control of military forces; as an integral part of a weapon or weapons system; or is otherwise critical to the fulfillment of intelligence or military missions. Consequently, although the new DFARS rule directs that the new supply chain risk contract clauses must be included in all IT solicitations, Section 806 authority will only apply to a subset of IT procurements.

Generally, Section 806 authority to exclude a source is limited to the heads of covered agencies, which the rule defines as the secretary of defense and the secretaries of the military departments, and may not be delegated below the level of the senior acquisition executive for each department. In addition, the interim rule sets out several prerequisites that must be satisfied before the DOD may exercise its Section 806 authority to exclude a source. To make a Section 806 exclusion, the DOD must:

- Obtain a joint recommendation by the under secretary of defense for acquisition, technology, and logistics and the chief information officer of the Department of Defense, concluding on the basis of a risk assessment by the under secretary of defense for intelligence that there is a significant supply chain risk;

- Determine, with the concurrence of the under secretary of defense for acquisition, technology and logistics, that (1) the exclusion is necessary to protect national security and (2) less intrusive measures are not reasonably available to reduce the supply chain risk; and

- Provide notice of the determination to the appropriate congressional committees.

The DOD's Section 806 authority to manage supply chain risk is authorized until Sept. 30, 2018.

[1] 78 Fed. Reg. 69268; 78 Fed. Reg. 69273.

Ronald Lee is a partner and Nicholas Townsend and Lauren Schlanger are associates in Arnold & Porter's Washington, D.C., office.