D

Impact of U.S. Government Cybersecurity Efforts on Contractors

Ronald D. Lee *and*
Nicholas L. Townsend
Arnold & Porter LLP

September 2011

IMPACT OF U.S. GOVERNMENT CYBERSECURITY EFFORTS ON CONTRACTORS

by
Ronald D. Lee and Nicholas L. Townsend

Information technology has revolutionized how we live our lives and how corporations, government, and the military work, but our dependence on this technology also creates vulnerabilities. Information technology is indispensible for most American businesses and the U.S.' military might relies on these technologies for command and control, communications, navigation, and intelligence.

As this year's high-profile cyber attacks on Sony, Google, Lockheed Martin, and the International Monetary Fund demonstrate, the threats are increasing in sophistication and the number of attacks is on the rise. At the same time, the United States is becoming more dependent on technology every day despite the growing cybersecurity risks. For example, the U.S. Army is currently working on a program to put smartphones in the hands of every soldier. These phones, most of which are manufactured outside the United States often in countries that are not U.S. allies, could introduce a host of new vulnerabilities. The National Security Agency is working on a more secure design for commercial smartphones and tablets that will be used by the military, but increased risk of cyber attacks is inevitable given the extraordinary pace of technological development, the globalized nature of the supply chain, and the government's increasing reliance on the Internet.

The Obama Administration has made confronting these challenges a priority by releasing an International Strategy for Cyberspace, proposing cybersecurity legislation, and publishing a Strategy for Trusted Identities in Cyberspace. The Department of Defense ("DoD") has also established its new Cyber Command and it has released the first DoD Strategy for Operating in Cyberspace. One of the five pillars in DoD's strategy is recognizing the importance of non-military networks maintained by private companies in supporting important military functions and committing to work with the Department of Homeland Security ("DHS") and the private sector to secure the defense industrial base and other critical infrastructure.

It is important for government contractors to understand how the government's efforts to address the growing risk of cyber attacks will impact their business. Two recent efforts are particularly relevant to government contractors:

(1) DoD's efforts to improve cybersecurity within the defense industrial base, including the DIB Cyber Pilot as well as new cyber incident reporting requirements and safeguards being considered for unclassified DoD information; and

(2) New efforts to manage supply chain risk, including provisions that give DoD special authority to exclude contractors who prose such risk.

I. DoD Defense Industrial Base Efforts to Improve Contractor Cybersecurity

The recent security breaches at RSA and Lockheed Martin have increased the intensity of DoD's efforts to secure information systems within the defense industrial base. However,

reducing the cybersecurity risk within the defense industrial base has been a DoD priority for years.[1]

Government contractors should be aware of two important new initiatives to secure the defense industrial base that could impact their businesses. First, DoD has issued a proposed rule that would require contractors to institute safeguards for unclassified DoD information in their systems and to report cyber incidents. Second, DoD has started a defense industrial base cybersecurity pilot to help contractors defend against cyber attacks. Each of these initiatives takes a different approach to improving cybersecurity and each could impact government contractors and their information systems.

A. Proposed Rule Requiring Contractors to Take New Steps to Protect Unclassified DoD Information and Report Cyber Incidents

DoD released a proposed rule on June 29, 2011 (the "Proposed Rule") that would add requirements for safeguarding unclassified DoD information and new cyber incident reporting requirements to the Defense Federal Acquisition Regulation Supplement ("DFARS").[2] These requirements are significant because they could create extra compliance obligations for any prime or subcontractor using, storing, or transmitting export controlled information or other nonpublic DoD information. These new requirements could impose substantial costs on small businesses that don't have the type of established information security procedures in place that many larger contractors do. Even sophisticated government contractors that have a facility security clearance and already comply with National Industrial Security Program Operating Manual ("NISPOM") requirements for classified information would have new reporting and safeguarding obligations for their unclassified networks under the Proposed Rule.

The Proposed Rule sets out two levels of protections – basic and heightened. Depending on the type of information involved, contract clauses requiring either basic or heightened security measures would be included in all solicitations and contracts that require a contractor or subcontractor to have nonpublic DoD information "resident on or transmitting through its unclassified information systems." Contractors would also have to put these provisions in any subcontracts that require access to such information.

i. Basic Security Requirements

Seven first-level security requirements would apply to any unclassified DoD information stored on, or transiting through, a contractor's information systems in order to protect against unauthorized disclosure, loss, or exfiltration.

---

[1] *See* DoD Instruction 5205.13, Defense Industrial Base (DIB) Cyber Security Information Assurance (CS/IA) Activities (Jan. 29, 2010); Directive-Type Memorandum (DTM) 08-027, Security of Unclassified DoD Information on Non-DoD Information Systems (July 31, 2009).

[2] DFARS Case 2011-D039, Proposed Rule, *Safeguarding Unclassified DOD Information*, 76 *Fed. Reg.* 36,089-95, (29 June 2011) (to be codified at 48 CFR pts. 204, 252).

(1) Unclassified government information may not be processed on public computers and such information cannot be posted on public websites that can be accessed without a password or another form of access control;
(2) The best level of security and privacy available must be used for transmitting electronic information, such as emails, text messages, and blogs;
(3) Reasonable assurances that access is limited to authorized recipients must be obtained when transmitting information via voice and fax;
(4) Information must be protected with at least one physical or electronic barrier, such as in a locked drawer/room or password protection;
(5) Electronic media that have been used to store unclassified information must be sanitized before disposal;
(6) Malware protection, including anti-virus and anti-spyware software, must be install and regularly updated and upgraded as necessary with patches, service packs, and hot fixes; and
(7) Subcontractor access to such information must be limited to those who have a need to know and employ requisite basic protections.

ii. Heightened Security Requirements

Three heightened security requirements would also apply to contractors who have seven types of information that require special handling, including information bearing designations indicating controlled access (e.g., For Official Use Only, Sensitive But Unclassified, etc.), Critical Program Information, personally identifiable information ("PII"), information subject to export controls under the International Traffic in Arms Regulations ("ITAR") and the Export Administration Regulations ("EAR"), and certain information exempt from mandatory public disclosure.

The three heightened requirements outlined below apply in addition to the basic requirements above.

(1) Information Security Program

Contractors must implement an information security program in unclassified information technology systems at the project, enterprise, or company-wide level. The specified National Institute of Standards and Technology ("NIST") Special Publication 800-53 minimum security controls must be employed. Specifically, contractors must comply with access control, awareness and training, contingency planning, maintenance, and system and communication protection standards set forth by NIST. If particular controls are inapplicable, the contractor must explain in writing why the NIST requirements do not apply.

(2) Authentication Credentials

Contractors may only use DoD-approved identity authentication credentials for authentication to DoD information systems.

(3) Cyber Incident Reporting

Within 72 hours of discovering a "cyber incident" that affects DoD information on, or transiting through, the contractor's unclassified information systems, the contractor would also be required to report the incident to DoD. Reportable "cyber incidents" include incidents involving possible data exfiltration or manipulation or other loss or compromise of DoD information on, or transiting through, the contractor's unclassified information systems, or any unauthorized access to an unclassified information system on which nonpublic DoD information is resident or transiting. Such incident reports would be made via a DoD website.

Contractors that are subject to these three heightened security requirements must report any cyber incidents regardless of whether the specific information involved in the incident falls into one of the special handling categories that require heightened safeguards. For example, unauthorized access to the unclassified information system of a contractor who is subject to the heightened safeguarding requirements could require an incident report, even if there is no evidence that any DoD information was compromised. Moreover, in many instances, the contractor may not know specifically what information was compromised at the time of the incident report and, in some cases, the contractor may never know the full extent of the breach.

Contractors would also be required to take certain actions in response to a cyber incident, including preserving images of affected information systems, conducting an immediate review of their unclassified networks for evidence of intrusion, and identifying any DoD information among the data accessed during the cyber incident. The contractor must also cooperate with the DoD Damage Assessment Management Office ("DAMO") to identify compromised systems.

iii. Potential Issues for Government Contractors

The Proposed Rule raises a number of potential issues for government contractors, in addition to the increased cost associated with implementing these news safeguards and reporting requirements. There are three potential concerns that may be of particular interest to contractors – (1) disclosure of information from cyber incident reports, (2) DoD use of cyber incident reports against contractors, and (3) the administrative burden associated with subcontractor compliance.

(1) Disclosure of Information from Cyber Incident Reports

Submission of cyber incident reports could create the risk of liability to third parties for disclosure of their information or contractors may incur substantial cost trying to obtain permission to disclose such third-party information. In cases where an incident report requires the contractor to disclose third-party data that is protected by a non-disclosure provision, the Proposed Rule specifies that the contractor must seek written permission from the owner of any third-party data to share the information with the government. Otherwise, a third-party, such as a customer or subcontractor, may have the right to sue the contractor for unauthorized disclosure.

There is also a risk that DoD may share threat information derived from incident reports with industry, which could result in a contractor's own proprietary data being disclosed to third parties. This could potentially put valuable business information at risk. Although the Proposed Rule places some limits on DoD's authority to disclose attribution information from cyber-

incident reports to third parties, it may disclose reported information that does not include attribution information at its discretion to assist other entities in protecting their information systems. This could include information about vulnerabilities, incidents, threats, or countermeasures. Moreover, any information submitted as part of an incident can be used in support of the government's ability to conduct law enforcement or counterintelligence activities, or other lawful activities in the interest of national security.

(2) DoD Use of Cyber Incident Reports Against Contractors

Negative information in a cyber incident report could harm the ability of the contractor who filed the report to win future DoD work if DoD concludes that the contractor has inadequate information security procedures that pose a cybersecurity risk. The Proposed Rule notes that reporting of a cyber incident itself will not automatically be assumed to be evidence that the contractor had inadequate information safeguards for DoD unclassified information. However, DoD reserves the right to consider such incidents in the context of an overall assessment of the contractor's compliance. This falls short of the fulsome safe harbor for cyber incident reporting that some contractors called for in their comments on the advance notice of proposed rulemaking that DoD released on March 3, 2010.

DoD may still be able to use cyber incident reports against contractors in a number of ways, despite the proposed rule's limits on use of incident reports themselves as evidence that the contractor has failed to provide adequate safeguards. For example, a cyber incident report could lead DoD to independently review the contractor's information security procedures, potentially resulting in:

- Termination of the contract for default;
- Demand that the contractor undertake expensive system upgrades, perhaps under threat of a government termination of the contract for default;
- Issuance of a Contracting Officer Final Decision ("COFD") that the contractor owes the government money, for example, as a credit to reimburse the government for the safeguards that were not provided;[3] or
- Negative assessment of the contractor's past performance in the Contractor Performance Assessment Reporting System ("CPARS"), which would also be available through the Federal Awardee Performance and Integrity Information System ("FAPIIS").

Therefore, a cyber incident report has the potential to negatively impact both the contractor's existing contracts and its ability to obtain future DoD work.

(3) Administrative Burden Associated with Subcontractor Compliance

The Proposed Rule puts the administrative burden of ensuring subcontractor compliance with these new safeguards on the prime contractor. The Proposed Rule would require prime contractors to include the relevant basic or enhanced security requirements in all subcontracts. Moreover, FAR Part 9.1 requires the prime contractor to affirmatively demonstrate responsibility for, among other things, proposed subcontractors. In order for such prime contractors to be

[3] 48 C.F.R. §§ 33.211, 32.604, 32.605.

determined responsible, they must have necessary "operational controls" and "technical skills" applicable to the prime contractor's products and services and those of its subcontractors, which would presumably include compliance with the new safeguarding requirements.[4] However, prime contractors generally have little to no control over, or insight into, their subcontractors' IT security protocols. Nevertheless, the Proposed Rule leaves only the prime contractor able to ensure that, at every tier, its subcontractors' IT safeguards comply with the Proposed Rule because there is no privity, or direct legal relationship, between the government and the subcontractor. Given the constant evolution of technology, and the ever increasing sophistication of cyber threats, the best way to ensure that the Proposed Rule is properly implemented is to provide appropriate training, education, updates, and resources to defend against cyber attacks and intrusions. This may impose substantial costs on smaller subcontractors and most prime contractors are likely ill equipped to police their subcontractors' investment in IT security and training.

B. DIB Cyber Pilot

In May 2011, DoD, in partnership with DHS, established a new Defense Industrial Base Cyber Pilot (the "DIB Cyber Pilot"), which takes a significantly different approach to mitigating the risk of cyber attacks on defense contractors than the Proposed Rule discussed above. The goal of this pilot is to provide defense contractors more robust protection for their networks by sharing classified threat intelligence and know-how about related network defense with the contractors and their commercial internet service providers ("ISP"). This threat intelligence allows the contractors and their ISPs to strengthen their existing cyber defenses.

The DIB Cyber Pilot has stopped hundreds of attempted intrusions by providing contractors the "special sauce" of malicious code signatures gathered from U.S. intelligence efforts, according to Deputy Secretary of Defense William Lynn.[5] However, the government is not monitoring, intercepting, or storing any private communications as part of the Pilot. It is only helping the companies or their ISPs identify and stop malicious activity so that they can defend their own networks.

The DIB Cyber Pilot is voluntary and approximately 20 companies are participating in the initial 90-day program. These reportedly include contractors, like Lockheed Martin, CSC, CAIC, and Northrop Grumman, as well as ISPs, such as AT&T, Verizon, and CenturyLink.[6] In August, Lynn said DoD and DHS plan to expand the Pilot to the rest of the industrial base in the

---

[4] 48 C.F.R. §§ 9.103; 9.104–1.

[5] Dep. Sec. of Defense W. Lynn III, Remarks at 2011 DISA Customer and Industry Forum (Aug. 16, 2011), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4863.

[6] Ellen Nakashima, NSA allies with Internet carriers to thwart cyber attacks against defense firms, Washington Post (June 16, 2011), *available at* http://www.washingtonpost.com/national/major-internet-service-providers-cooperating-with-nsa-on-monitoring-traffic/2011/06/07/AG2dukXH_print.html.

future. The DIB Cyber Pilot is the beginning of something bigger, according to Lynn, who said it would serve as a model that can be transported to other critical infrastructure sectors by DHS. [7]

In contrast to the Proposed Rule that requires contractors to report cyber incidents to the government, the primary flow of information in the DIB Cyber Pilot is from the government to contractors. This approach is cost effective because the government is leveraging existing infrastructure to provide contractors substantial additional protections at a fractional increased cost. Although the Pilot is a more innovative public private model for sharing information than the more traditional approach of the Proposed Rule where the government sets security standards and imposes reporting requirements, it is possible that these two different approaches could support each other in the future. For example, the government could add what it learns from the Proposed Rule's cyber incident reports into the DIB Cyber Pilot's "secret sauce" of cyber threat intelligence in order to provide better threat information to its industry partners in the future.

II. Supply Chain Security

The global nature of modern supply chains has reduced costs, but it also has the potential to introduce risk because critical components of systems the U.S. relies on are manufactured overseas with little oversight, often in countries that are not U.S. allies. Fears have been growing within Congress, DoD, and the intelligence agencies that technical components from overseas, such as microchips and telecommunications equipment manufactured in China, could expose critical U.S. systems to cyber attacks. For example, Senator Jon Kyl (R-Ariz.) and seven other senators expressed concerns in 2010 that China-based Huawei's potential role as a supplier to Sprint Nextel could create substantial risk for U.S. companies and possibly undermine U.S. national security. Such fears are inflamed by incidents like the 2010 federal prosecution that exposed more than 59,000 counterfeit microchips from China that were sold by VisionTech Components to the U.S. Navy and other U.S. customers for use in military warships, fighter planes, missiles, and missile defense systems. These concerns about supply chain security have grown out of a series of reports calling attention to increased supply chain risk, including DoD's December 22, 2009 report on trusted defense systems and the January 2010 report by the Bureau of Industry and Security at the Department of Commerce on counterfeit electronics. The government's growing concerns about cybersecurity risk arising from the role of foreign manufacturers in the supply chain are important for government contractors to understand when choosing their suppliers.

A. Section 806 of the Ike Skelton National Defense Authorization Act

On July 6, 2011, a new law went into effect that gives DoD the authority to address the risk that a company in the supply chain for a national security system could sabotage the system's operations. The Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (the "Act"), which President Obama signed into law on January 7, 2011, contains new provisions enhancing the authority of the Secretary of Defense and the Secretaries of the military departments (collectively, the "Secretary") to take certain adverse procurement actions if the

[7] Dep. Sec. of Defense W. Lynn III, Remarks at the 28th Annual International Workshop on Global Security (Jun 16, 2011), *available at* http://www.cybersecuritymarket.com/2011/06/16/defense-industrial-base-dib-cyber-pilot/.

Secretary determines that a company poses a risk to supply chain security for a national security system.[8] The adverse actions permitted under Section 806 of the Act include the potential exclusion of a company from a procurement. The Act also requires DoD to inform other federal agencies that may be affected by similar supply chain risk of its decision to exclude a contractor.

(i) When Does Section 806 Apply?

Section 806 applies to certain procurements for "national security systems" and items for use in such systems. A "national security system" is an information system, including a telecommunications system, that is used: (1) for intelligence activities or cryptologic activities related to national security; (2) for command and control of military forces; or (3) as an integral part of a weapon or weapons system.

The statute aims to minimize risks to the supply chain for national security systems — that is, the network of organizations, people, technology, activities, information, and resources a contractor relies on to deliver to DoD a national security system or a component of such a system. Section 806 defines a "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."

Section 806 authorizes the Secretary to take adverse action when the terms of the solicitation or contract require the procuring agency to consider potential risk to the supply chain. Specifically, the statute applies to: □

- A source selection where the solicitation contains a performance specification or an evaluation factor relating to supply chain risk;
- The consideration of proposals for and issuance of a task or delivery order where the task or delivery order contract has a requirement relating to supply chain risk; or
- Any contract action involving a contract for a national security system that includes requirements relating to supply chain risk.

(ii) Potential Adverse Actions

The Act authorizes the Secretary to take adverse action against a contractor to protect national security by reducing supply chain risk. These adverse actions — characterized in the statute as a "covered procurement action"— include the exclusion from a procurement of a contractor that poses an unacceptable risk to supply chain security. Alternatively, the Secretary may direct a prime contractor not to use a particular subcontractor that poses an unacceptable risk.

---

[8] Ike Skelton National Defense Authorization Act for Fiscal Year 2011, H.R. 6523, 111th Cong. § 806 (2010).

The Secretary must complete three steps in order to take an adverse action under the Act to exclude a source:□

- Obtain a joint recommendation from the Under Secretary of Defense for Acquisition, Technology, and Logistics and DoD's Chief Information Officer, concluding that there is a significant supply chain risk. This conclusion must be based on a risk assessment by the Under Secretary of Defense for Intelligence.
- Determine, with the concurrence of the Under Secretary of Defense for Acquisition, Technology, and Logistics, that:
  (a) the exclusion is necessary to protect national security; and
  (b) less intrusive measures are not reasonably available to reduce the supply chain risk.
- Provide notice of the determination to the appropriate congressional committees.

(iii) Limited Disclosure of the Basis for Exclusion

The Secretary may limit disclosure of information relating to the basis for a contractor's exclusion. In order to do so, the Secretary must determine that the risk to national security from disclosure of the information outweighs the risk due to nondisclosure.

Once the Secretary exercises its authority to limit disclosure of information relating to an exclusion, the Act limits review of the Secretary's actions. Section 806 provides that if the Secretary "has exercised the authority…to limit disclosure of information…no action undertaken by [the Secretary] under such authority shall be subject to review in a bid protest before the Government Accountability Office [GAO] or in any Federal court." It is unclear whether this provision precludes only review of the Secretary's action to withhold information relating to an exclusion, or precludes bid protests challenging the exclusion action. Ultimately, even if the review limitation precludes review only of the Secretary's withholding of information, this limitation still significantly inhibits a contractor's ability to protest an exclusion because the adjudicator likely cannot compel disclosure of withheld information needed to evaluate the propriety of an exclusion.

(iv) DoD Disclosure of Exclusion to Other Federal Agencies

The Act also provides that the Secretary "shall 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" of DoD's exclusion under Section 806. Accordingly, although Section 806 only applies to DoD, DoD will inform other relevant agencies of an adverse action taken against a contractor, which will likely limit that contractor's ability to obtain work from other parts of the U.S. government as well.

B. Extension of Supply Chain Security Provisions to the IC

A provision based on Section 806 of the Act has been included in Section 309 of the Senate's Intelligence Authorization Act for Fiscal Year 2012, S. 1458, (the "Bill"). Section 309 would give non-DoD components of the Intelligence Community ("IC"), such as the Central Intelligence Agency or the Office of the Director of National Intelligence ("DNI"), authority to

address the risk that a company in the supply chain for a national security system could sabotage the system's operations.

Section 309 of the Bill is substantially similar to Section 806 of the Act. In fact, the Senate committee report on the Bill specifically states that "Section 309 is based on Section 806 of the Ike Skelton National Defense Authorization Act for fiscal year 2011 (Public Law 111-383)" and the provision in Section 309 would expire in January of 2014 at the same time as Section 806 of the Act. However, the provisions in Section 309 have been adapted for the IC. For example, Section 309 only requires that IC agencies notify the DNI of exclusions, instead of the broader notifications that DoD must make to other federal agencies. Nor does Section 309 contain a provision that pertains to review in a bid protest before GAO or the Court of Federal Claims.

The House intelligence authorization legislation for 2012, H.R. 1892, contains a similar supply chain security provision in Section 308. The only substantive difference between the House and Senate legislation is a provision in H.R. 1892 that ensures that these special supply chain risk authorities cannot be delegated below the level of a service acquisition executive. According to Representative Rogers who proposed the amendment, the change reflects Congress' understanding that these acquisition authorities will not be used lightly and that all decisions under this provision will be carried out by responsible senior officials within the intelligence community and coordinated and overseen by the Director of National Intelligence.

The House of Representatives passed H.R. 1892 on September 9, 2011 and the Senate is expected to take up the measure later this year. The Senate Select Committee on Intelligence also reported S. 1458 to the full Senate, but the Senate has not voted on it yet.

This IC specific version of Section 806 is significant in that it demonstrates continuing interest from both Congress and intelligence agencies in increasing the tools available to address the growing problem of supply chain risk.

C. Supply Chain Risk in Civilian Agencies

The government's efforts to manage supply chain risk are not limited to agencies with a national security mission. For example, a working group, which includes members from NIST and the State and Homeland Security Departments, is preparing a set of proposed best practices to address supply chain risk in the unclassified community. The working group's efforts build on concepts and best practices that DoD and DHS developed for the Comprehensive National Cybersecurity Initiative.

As part of this effort, in 2010, NIST proposed a set of best practices to manage supply chain risk.[9] The practices are intended to apply to systems rated as high impact under the Federal Information Processing Standard 199 scheme for assessing risk. The recommendations

[9] M. Swanson, N. Barton, R. Moorthy, National Institute of Standards, Piloting Supply Chain Risk Management Practices for Federal Information Systems, Draft NISTIR 7622 (Jun. 2010), *available at* http://csrc.nist.gov/publications/drafts/nistir-7622/draft-nistir-7622.pdf.

in NIST's draft interagency report entitled "Piloting Supply Chain Risk Management Practices for Federal Systems" pull together design, development and acquisition practices already in place that could apply to managing risk in the supply chain. In developing the recommendations, the working group focused on practices that are already available and could be readily implemented at a reasonable cost.

Once the practices have been evaluated in operation, NIST plans to expand its draft report into a special publication to provide guidelines to agencies. NIST had originally planned to release a "final version" of the report in early 2011 followed by a "first public draft of the special publication" later in the year, but neither has been released to date.

Although the best practices in NIST's report are largely focused on federal agencies, they still provide a useful roadmap for government contractors seeking to manage their own supply chain risk. The report can help contractors understand the government's expectations in this evolving area.