LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Government Contracts Practice February 11, 2014 | Number 1645

Government Procurement: Increased Security Scrutiny in IT Supply Chains

New laws and regulations require contractors who supply information technology in their products to control supply chain risk.

The US Government (USG) has adopted a series of laws and regulations that focus increased scrutiny on the security of supply chains for information technology (IT) procured for government use. These laws and regulations will impose new obligations on contractors to understand their full supply chains (particularly to the extent of any significant foreign sourcing) and to create legal and operational mechanisms to address and control security risks that might arise from characteristics of their supply chains. These laws and regulations may also affect decisions regarding mergers and acquisitions that involve government contractors, particularly in cross-border transactions.

Summary of Laws and Regulations

In 2008, President Bush issued the Comprehensive National Cybersecurity Initiative (CNCI) to address the growing threat of cyber intrusions and attacks on US networks, both within government and in critical infrastructure.[1] One of the CNCI's key recommendations focused on the risk that IT supply chain exploitation could be used to launch such intrusions and attacks: **"Initiative #11. Develop a multi-pronged approach for global supply chain risk management.** …Risks stemming from both the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services."[2]

Congress and Executive Branch agencies have recently enacted laws and regulations that implement the policy expressed in Initiative #11 of the CNCI:

DFARS Interim Rule 2012-D050

Section 806 of the 2011 National Defense Authorization Act provided specific authority for the US Department of Defense (DOD) to address IT supply chain risk in procurements conducted by DOD. DOD took no action on this statutory authorization until November 18, 2013, when it adopted Interim Rule 2012-D050 as a provision of the Defense Federal Acquisition Regulations Supplement (Interim Rule). DOD took the unusual step of adopting 2012-D050 as an interim rule rather than a proposed rulemaking, with the comment period coming after adoption (comments closed January 17, 2014). DOD implemented the rule in this fashion in part because the underlying Section 806 statutory authority sunsets in 2018; the authority is a "pilot program" whose results will be assessed in 2017.

The Interim Rule requires that for any DOD acquisition involving "the development or delivery of any information technology, whether acquired as a service or as a supply," DOD must consider the need to include "supply chain risk" as an evaluation in award of contracts (broadly defined). Supply chain risk is the risk that an adversary may surreptitiously embed or exploit a capability to surveil or sabotage the

function or operation of an IT system that is: (1) used in signals or intelligence activities, command and control of military forces; or that is (2) an integral part of a weapon or weapons system or critical to direct fulfillment of military or intelligence missions. While not explicit in the Interim Rule's definitions, an "adversary" implicitly is a foreign person (whether inside or outside the US)

The scope of the Interim Rule is broad enough to apply to virtually every component (hardware and software) in all networks or systems used by DOD. The Interim Rule specifically covers "commercial-off-the-shelf" (COTS) products that are sold directly to DOD as well as any equipment and components used by a vendor that provides "services" to DOD, where such IT equipment would be integral to the service (*e.g.*, managed network services). Subject to a variety of procedural safeguards — including the requirement that the authority granted is to be exercised at very senior levels of Government, without delegation — the Interim Rule authorizes DOD to:

- Exclude a source that fails to meet qualification standards from an award, for the purpose of reducing supply chain risk
- Exclude a source that fails to achieve an acceptable rating with regard to an evaluation factor relating to supply chain risk from an award
- Withhold consent for a contractor to subcontract with a particular source from consideration

Under express statutory authority, the Interim Rule provides that DOD can take these steps without disclosing any facts concerning the action or the basis for the action to the contractor, and without review of its decision in a bid protest. The Interim Rule does require, in addition to very senior decisionmaking, considerable fact-finding and reporting. While these requirements may constrain widespread enforcement, the consequences of potential enforcement can be severe and may therefore establish de facto industry standards and best practices.

The Interim Rule does not provide specific standards by which contractors and vendors can assess their supply chain risk posture, but instead "leaves it up 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." Thus, while the Interim Rule does not impose specific burdens on contractors seeking to comply, and accordingly offers some flexibility, neither does the rule provide any "best practices" or "safe harbor" on which contractors can rely to avoid exclusion or other discretionary remedies.

Intelligence Community Directive 731

On December 7, 2013, the Director of National Intelligence issued Intelligence Community Directive 731 (ICD 731). ICD is very similar to the Interim Rule (above) in that ICD 731 directs all member agencies of the Intelligence Community to consider supply risk in IT procurements and provides that agencies need not disclose the basis for disqualifying a putative contractor based on supply chain risk. ICD 731 states: "[W]hen acquiring IT products, contractors, subcontractors, or vendors may be excluded from competing based on supply chain risk factors identified in [a] risk assessment. The disclosure of that exclusion may be limited when necessary to protect national security."

ICD 731 also establishes procedures for sharing supply chain threat information and risk management best practices across the Intelligence Community.

"Wolf Provision"

On January 17, 2014, the Consolidated Appropriations Act of 2014 was signed into law, providing funding for the US Departments of Justice and Commerce, the National Aeronautics and Space Administration, and the National Science Foundation. Section 515 of the Act (the Wolf Provision, after its author, Representative Frank Wolf (R-VA)) restricts spending by those agencies on any "high-impact" or "moderate-impact" information system or network until a supply chain risk assessment has been performed on the to-be-procured IT technology.[3] The agencies are to assess "risk associated with such system[s] being produced, manufactured, or assembled by one or more entities identified by the United States Government as posing a cyber threat, including but not limited to, those that may be owned, directed, or subsidized by the People's Republic of China." The agencies are to coordinate with the Federal Bureau of Investigation "and other appropriate agencies" to obtain threat information for such assessments (presumably classified threat information).

The affected agencies are in the process of formulating regulations to implement the Wolf Provision, but clearly as a consequence of this enactment, the evaluation of supply chain risk in a wide array of procurements is not just permitted, but mandated by statute.

Potential Issues

Taken together, the Interim Rule, ICD 731, and the Wolf Provision create a variety of potential difficulties for contractors providing services to those USG agencies identified above — both in terms of new hurdles to winning and performing USG contracts as well as potential liability risks. We highlight here some of the most prominent issues:

- **Technology Origin "Catch-22"** Revelations from Edward Snowden regarding alleged exploitation of IT equipment (both of US and foreign origin) for surreptitious electronic surveillance by US and British intelligence agencies has placed competing pressures on US IT vendors and suppliers. Under the trio of legal provisions discussed herein, contractors and vendors will feel pressure to eschew use of hardware and software components from countries such as China in order to address supply chain risk and win USG business. However, many contractors and vendors now report concerns expressed by their non-US customers about the use of US-centric IT supply chains because of the worry that US technology has been compromised by the USG. We believe this "Catch 22" may become more prevalent as the supply chain requirements discussed above are implemented and enforced by the USG.

- **Lack of Recourse** A decision by any agency that a contractor or vendor should be excluded from procurement activities based on supply chain risk may impair all of that business' USG contracting opportunities. All three provisions contemplate information sharing on the supply chain risk issues between agencies. Because exclusion cannot be challenged via bid protest and the USG is allowed to keep the basis for exclusion confidential, excluded contractors will have no process by which they can challenge their disqualification.

- **Potentially Broad Consequences** Because of the potentially confidential nature of USG review and evaluation process, an excluded contractor or vendor may receive little or no information about what hardware or software components triggered the negative supply chain risk analysis. This may be especially difficult for US-based contractors who would otherwise seemingly pose no supply chain risk, other than inclusion of potentially a single component that causes concern. These three provisions do not necessarily provide guidance or a mechanism for contractors to improve their supply chains by ferreting out "risky" components. Contractors may accordingly have limited information about potential risks and evaluated deficiencies in their supply chains — and

corresponding limits on their abilities to improve the security of their supply chains through precisely targeted action.

- **Possibly Risky Partnerships** Even contractors or vendors who believe they can deduce what risk is causing negative evaluation of their supply chain may face significant challenges in solving their problem. A teaming agreement partner or subcontractor who seems to be the probable source of the risk may not acquiesce in its replacement without evidence that identifies the contractor as the problem. Further, the USG may be unwilling to confirm facts needed to supply that evidence. Thus, parties in exclusive arrangements, or subject to contractually-agreed constraints on competing, may find themselves tethered to a disqualifying risk.

- **Ambiguity Around Foreign Worker Status** The trio of legal provisions do not provide guidance on whether using, for example, a foreign citizen living and working in the US under a work visa would cast a taint on software or firmware developed by that foreign person. An interpretation that extends the scope of these rules to personnel as well as components would be a significant expansion.

- **Potentially Higher Costs from Reduced Suppliers** While the USG can and should impose supply chain security as a criterion for procurement decisions, as a potentially unintended consequence — in order to comply with these provisions, contractors and vendors may need to dramatically shrink their sources of supply, particularly given the extensive amount of technology being developed in countries like China. A shrinking source of supply may drive costs of IT technology for the USG up — and such price increases may spill beyond just USG procurement because of the additional costs and operational difficulties in having one supply chain for USG products and one for other commercial customers. In addition, the shrinking pool of acceptable suppliers may shrink the scope of leading-edge technology available to the USG, especially to the extent IT innovation emanates from countries like China and India. A rise in the cost of IT technology and the decrease in access to potentially cutting edge technology may lead to less robust USG networks, which itself could be a security issue for both the USG and its contractors.

In addition to their potential effects on USG procurement, these supply chain laws and regulations could impact cross-border mergers and acquisitions that involve USG contractors. Such transactions have typically been reviewed by the Committee on Foreign Investment in the US (CFIUS), and CFIUS already has authority to address supply chain risk arising from an acquisition as needed. To the extent that certain foreign acquirers are deemed likely to expose US contractors to supply chain risk if the foreign acquirers integrate vertically, in certain circumstances, CFIUS may be inclined to impose supply chain-related “mitigation conditions” in a wider range of reviewed transactions, in an effort to reduce risks of loss of source of supply for key USG technology missions.

Even if such constraints are not directly imposed, government contractors and their prospective foreign acquirers will need to take a much closer look at whether international transactions will inject supply chain risk into a particular business or product, thereby risk ing loss of USG contracting revenue as a result of their transaction.

While no one will be immune, the risks described above are likely to be particularly acute for particular categories of contractors and subcontractors. Those who supply cutting-edge or sensitive information systems, products, or services, particularly from jurisdictions perceived as high-risk (or whose supplies are from such jurisdictions) will need to be most vigilant.

Considerations for Affected Vendors and Contractors

Because these three legal provisions relating to supply chain risk are just now being implemented, whether or not the USG will wield them sparingly or expansively remains to be seen. In either case, government contractors (whether prime or sub) and suppliers (hardware, software or services) may consider a number of proactive measures:

- **Supply Chain Transparency** Contractors and vendors should consider aggressive and on-going "know your supplier" programs so that they can know and identify their full supply chain stack. Simple transparency (auditing and ongoing maintenance of transparency) may be enough to help contractors address supply chain risk issues before they come to the USG's attention. Such programs are already advisable to respond to other USG efforts to assure the supply chain (such as new regulations on avoiding counterfeit parts, issued pursuant to the 2012 National Defense Authorization Act).

- **Flexible Relationships** Contractors and suppliers should carefully consider teaming, partnering, joint venture and sourcing agreements (including subcontracts) from a supply chain perspective and may consider implementing mechanisms to allow supply chains to be adjusted if there is a negative USG supply chain outcome.

- **Supplier Options** As a matter of good business practice, contractors should have a range of alternative suppliers (if feasible) in order be unfettered if one supplier is found to pose supply chain risk.

- **Proactive Response** Contractors may consider proactively conducting supply chain audits and using third-party attestations regarding supply chain posture when bidding on USG procurements, as a way of proactively addressing these new laws and regulations.

- **Due Diligence in Transactions** In the transaction context, parties to a merger or acquisition that touches USG contracting should be conscious of supply chain risk as a material due diligence point of focus, with a particular focus on supply chain visibility in order to assess deal risk.

Given the stakes in government contracting and the potential downside for businesses using or acquiring potentially risky suppliers, IT companies should consider the new security regulations as soon as possible.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Edward J. Shapiro
edward.shapiro@lw.com
+1.202.637.2273
Washington, D.C.

Christopher Simkins
CEO of Chain Security LLC
+1.571.354.0068

Chain Security specializes in assessing and mitigating security risks that originate in telecommunications and information technology supply chains.

Endnotes

---

1 *See* http://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

2 *See* http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (emphasis in original).

3 Section 515 is a successor to a previous version of the provision that was included in the Consolidated and Further Continuing Appropriations Act of 2013. The successor provision was found in Section 516 of the 2013 Act.