crowell moring

CLIENT ALERT

Supply Chain Perspectives — Connecting the Dots on Supply Chain Security and Risk Management

Dec.02.2019

In this installment, we track how the push to ensure the security of the federal procurement supply chain continues to mature and expand rapidly, as new mandatory reporting obligations are imposed and other proposed regulations are introduced, restrictions on telecommunications equipment from certain Chinese entities deemed a security risk are beginning to be implemented, and cybersecurity moves one step closer to becoming a prerequisite to bidding on federal contracts.

New, Mandatory Obligations to Report Counterfeit and Nonconforming Goods

As we highlighted earlier this week, a new FAR clause finalizes a FAR provision that dramatically expands the mandatory reporting of counterfeit and certain nonconforming parts to the Government-Industry Data Exchange Program (GIDEP) and, in some instances, the relevant contracting officer. Representing a significant expansion of the existing DFARS 252.246-7007, the new rule applies the prospect of GIDEP reporting to all contractors of all federal agencies, where such contractors identify electronic and non-electronic counterfeit parts, as well as other nonconforming parts, in their supply chains. Unlike the rule as proposed in 2014, however, the final rule explicitly excludes procurements for commercial items, medical devices subject to FDA reporting, and commercially-available off-the-shelf items. Despite such significant "de-scoping," the rule should be expected to present significant challenges to civil and defense contractors alike when the reporting rule goes into effect on December 23, 2019.

Department of Commerce Proposes Information Technology Supply Chain Regulation

The Department of Commerce has proposed regulations, *Securing the Information and Communications Technology and Services Supply Chain*, that would allow the government to review transactions involving the acquisition, import and/or installation of information technology and services involving property of a foreign country or national. This proposed regulation invokes supply chain management concerns due to the far reaching impact the rule, once enacted, would have on companies and their suppliers where the government cites a risk of sabotage to U.S. information technology or national security concerns.

DoD Release of Cybersecurity Maturity Model Revision 0.6

The Department of Defense (DoD) recently released yet another revision to the highly anticipated Cybersecurity Maturity Model Certification (CMMC). The CMMC will require all contractors doing business with the DoD to obtain a cybersecurity certificate ranging from Level 1 – 5 in order to be eligible for contract awards. The applicable CMMC level, and associated stringency of

cybersecurity requirements, will be determined by contract-specific "go/no-go" solicitation criteria. Revision 0.6 offers industry a preview of the nearly completed CMMC regulatory landscape for Levels 1 – 3, since the final version of the CMMC is expected at the end of January 2020. This revision provides helpful insight into the requirements for Level 3, which notably contain requirements beyond NIST SP 800-171, the cybersecurity standard for DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. Levels 4 – 5 will be the subject of another revision this year, but they currently contain important supply chain management and monitoring requirements. Industry can utilize this current CMMC draft revision to self-assess their cyber hygiene and identify areas of improvement that may be necessary to be eligible for DoD contract opportunities in 2020.

2019 NDAA Section 889: Covered Telecommunications Panel Discusses Supply Chain Impact

The General Services Administration (GSA) held a robust discussion on November 6, 2019, with industry panelists regarding the 2019 NDAA Section 889 prohibition on covered telecommunication products and services, which has been implemented as an interim rule with immediate effect (FAR 52.204-24 and FAR 52.204-25) and rolled out by GSA in mass "bilateral" modifications. The panel focused on the legal risks and supply chain impact to companies once Section 889 (a)(1)(B) is implemented on August 13, 2020. The (a)(1)(B) provision prohibits the Government from entering into a contract, or extending or renewing a contract, with an entity that uses certain covered telecommunications equipment or services.

The panel discussed the far reaching impact of the (a)(1)(B) prohibition since the prohibition applies company-wide to a contractor's "use" of covered telecommunications, and is not limited to performance of government contracts. The supply chain was identified as a particular risk, since contractors will be responsible in flowing down the Section 889 requirements and ensuring no covered telecommunications are used throughout a subcontractor or supplier's business operations. The panel agreed that covered telecommunications are not restricted to specific products, but could transcend to any area of business operations where technology is utilized containing covered telecommunications.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Adelicia R. Cliffe
Partner – Washington, D.C.
Phone: +1 202.624.2816
Email: acliffe@crowell.com

Peter Eyre
Partner – Washington, D.C.
Phone: +1 202.624.2807
Email: peyre@crowell.com

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Nicole Owren-Wiest
Partner – Washington, D.C.
Phone: +1 202.624.2863
Email: nowrenwiest@crowell.com

Paul Freeman
Senior Counsel – New York
Phone: +1 212.895.4251
Email: pfreeman@crowell.com

Michael G. Gruden, CIPP/G
Associate – Washington, D.C.
Phone: +1 202.624.2545
Email: mgruden@crowell.com