crowell moring

CLIENT ALERT

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

Aug.22.2019

In this installment, we begin with a series of recent developments that—when threaded together—provide a vivid illustration of the challenges that are gathering on the horizon for defense contractors. Born out of the intersections of the False Claims Act and the continuing pressure to eliminate gaps in supply chain security, the risks highlighted below warrant a reexamination of how contractors define, investigate, and consider disclosure of potential gaps in supply chain security.

Defense Contractors Increasingly Must Confront the Risk of Exposure to False Claim Liability for Known Gaps in Security

On July 31, 2019, Cisco Systems agreed to pay $8.6 million to settle allegations in United States ex rel Glenn, et al v. Cisco Systems, Inc. that the company violated the False Claims Act (FCA) by selling video surveillance systems to state and federal agencies containing gaps in the security of the software in those systems. Significantly, the recovery secured by the relator in that case was based upon security gaps only, and, in fact, though Cisco is alleged to have known about those potential gaps in security, there was no evidence—*nor allegation*—that such gaps were actually exploited or that the security of the products sold to the government was ever compromised.

As Mark Chandler, Cisco's Chief Legal Officer, observed in a blog post discussing the settlement, customer "expectations have changed," and "what seemed reasonable at one point no longer meets the needs of our stakeholders today." Put another way, in the current climate contractors should anticipate that their government customers will increasingly view products that may pose a security risk as non-conforming.

Gaps and Other Risks to Supply Chain Security Will Continue to be Identified

Yet, as defense contractors remain in the early stages of implementing the wave of federal cybersecurity contracting requirements, it is apparent that such gaps arguably no longer meeting the government customer's rising expectations may still remain commonplace. As members of the Crowell Supply Chain Team explained recently, an audit by the Department of Defense Inspector General (DODIG) found that contractors are not consistently implementing cybersecurity standard NIST SP 800-171, despite being required to do so under DFARS 252.204-7012.

And while the DODIG audit did not assess compliance in the supply chain, as those requirements of the DFARS Safeguarding Rule are in fact flowed down to the defense industrial base supply chain, and increasingly subjected to oversight and audit by prime contractors and the Defense Contract Management Agency alike, the number of instances of non-compliance with DFARS 252.204-7012 and corresponding gaps in supply chain security known to prime defense contractors and their suppliers should be expected to proliferate.

Defense Contractors Will be Well Served by Taking a Fresh Look at How These Risks are Defined and Managed Proactively

The intersection of these recent developments implicates important questions for defense contractors as they implement, flow-down, and oversee progress towards aligning the security of their supply chains with rapidly evolving government contracts requirements. In particular, as contractors identify potential gaps in security flowing through their examination of and work with suppliers, consideration should be given to whether such gaps might fail to achieve compliance with the underlying contract, and, in so doing, could be indicative of the presence of "credible evidence" of a civil false claim for purposes of the Mandatory Disclosure Rule under FAR 52.203-13. This is particularly important where, as in the current environment, the window may be closing on the ability to treat risks to supply chain security as "garden variety" instances of "minor" contract noncompliance. *See Universal Health Servs., Inc. v. United States ex rel. Escobar*, 136 S. Ct. 1989, 2003 (2016). As a consequence, during this very fluid time, fresh consideration should be given to when and under what circumstances gaps that may be identified by security or procurement organizations are, in turn, the subject of a legal investigation, and whether a contractor's internal thresholds for disclosing such gaps to the government customer is warranted from a risk management perspective.

And finally, ICYMI:

- Earlier this month, the FAR Council published an interim rule, FAR Subpart 4.21, effective immediately, implementing a portion of section 889 of the FY 2019 National Defense Authorization Act, specifically, the ban on government procurement of any equipment, system or service that uses covered telecommunications equipment or services from certain Chinese companies, particularly any telecommunications equipment or services from Huawei or ZTE (or any affiliate) and certain video surveillance and telecommunications equipment or services from three other Chinese companies (or their affiliates).

- The National Institute of Standards and Technology (NIST) updated the Risk Management Publication Schedule, which announced delays in the release of several key cybersecurity publications due to the regulatory review cycle of the Office of Management and Budget (OMB). Specifically, the release of NIST SP 800-171, Rev. 2 and the much anticipated NIST SP 800-171**B**, which features the new standard for *Enhanced Security Requirements for Critical Programs and High Value Assets*, are both on hold. The delay is attributed to OMB currently reviewing NIST SP 800-53, Rev. 5 since both NIST SP 800-171 standards depend on certain NIST SP 800-53 controls.

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

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

Judy Choi
Counsel – Washington, D.C.
Phone: +1 202.624.2954
Email: jchoi@crowell.com

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

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