A Secure Supply Chain Is a Competitive Advantage

Government Contracts

More than ever, federal contractors are being held responsible for the security of their supply chains—and the pressure is growing. This is especially true for those supporting the military and intelligence communities, as adversaries seek to launch novel, asymmetrical attacks on the most vulnerable points in the defense-industrial base.

"The price of failure is steep," says Adelicia Cliffe, a partner in Crowell & Moring's Government Contracts Group. "Those contractors unwilling to invest in supply chain security risk not only failing to keep up with the avalanche of new regulatory requirements, but, even more important, missing a great opportunity to seize a distinct competitive advantage."

Concerns about the exposure of contractor supply chains to a variety of threats—such as exfiltration of valuable information, attacks on critical infrastructure systems, counterfeit parts, and software manipulation to access government or contractor systems—aren't new. But they've taken on greater urgency in the past few years following the publication of an influential report, The MITRE Corp.'s "Deliver Uncompromised." Citing the changing nature of war and the criticality of securing the supply chain, the report's authors advocated that supply chain security become a top priority of the defense contracting process.

Shortly thereafter, the Department of Defense announced its intention to implement the strategy and started a pilot program that would place a contractor's overall security on par with cost, performance, and meeting deadlines as key procurement criteria.

A Shifting Landscape

The upshot is that the U.S. government is moving to tighten contractor security requirements through new statutes, regulations, and agency guidance. Cliffe observes that "while contractors have historically built their supply chains with cost, performance, and schedule in mind, now security has to be top of mind."

Numerous legislative and regulatory steps have been implemented or are in the works to strengthen the supply chain on multiple fronts. Among the most noteworthy:

Tighter cybersecurity. A draft of a new standard by the National Institute of Standards and Technology would protect "controlled unclassified information," which contractors and subcontractors typically must handle, against "advanced persistent threats." In addition, DoD is formalizing a certification process to ensure that contractors meet cybersecurity requirements. Attaining a specified level of certification would, for the first time, be a prerequisite for bidding on contracts.

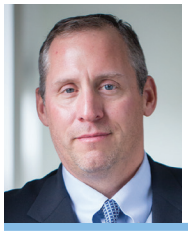
Exclusion of specific non-U.S. suppliers. A 2018 Federal Acquisition Regulation (FAR) rule prohibited the use of hardware, software, and services from the Russian firm Kaspersky Labs, and a 2019 interim FAR rule banned government procurement of telecommunications equipment or services from Chinese giants Huawei and ZTE.

Reporting of counterfeit and nonconforming parts. A new FAR rule requires contractors to report certain counterfeit (or suspected to be counterfeit) parts and certain nonconforming parts to the Government-Industry Data Exchange Program.

GSA standards. The General Services Administration has proposed the adoption of tougher supply chain risk management standards for government procurement of information and communications technology systems.

NDAA requirements. Recent National Defense Authorization Acts continue to drive the development of even more supply

"While contractors have historically built their supply chains with cost, schedule, and performance in mind, now security has to be top of mind." **Adelicia Cliffe**



"Contractors that don't have a firm grasp on their supply chains' security won't be positioned to compete effectively for government business." **Paul Freeman**

chain imperatives, including those requiring:

- Creation of a Supply Chain and Counterintelligence Risk Management Task Force (2020).
- Establishment of disclosure obligations and prohibitions where there is risk of foreign-government influence over products and services (2019).
- Integration of supply chain risk management into DoD's acquisition decision cycle (2018).

The Stakes Are Higher

It's clear that contractors will have their hands full trying to keep up with the rising tide of security requirements. And the stakes of compliance are getting higher, says Paul Freeman, senior counsel in Crowell & Moring's Government Contracts Group. "Contractors are being evaluated by their ability to protect their supply chains," he says. "They're more directly responsible for ensuring that subcontractors know about and meet security requirements, and they're legally obligated to report actual and potential security problems in their chains. Those that don't have a firm grasp on their chains' security won't be positioned to compete effectively for government business."

Judy Choi, a counsel in Crowell & Moring's Government Contracts Group, adds that pressure is mounting on contractors from many directions. "Standard contractual terms are changing as agencies roll out new initiatives to stay on top of these issues in addition to the new FAR and DoD FAR Supplement requirements. We also anticipate increased focus on supply chain issues from relators and whistleblowers, which should prompt more litigation."

Freeman expects that the challenges posed by the recent legislative and regulatory steps will be subject to further scrutiny in two instances: where early cases show courts' willingness to uphold agency procurement decisions based on supply chain security concerns, and where the growing importance of security in procurement implicates other legal regimes triggered by concerns that the government isn't getting what it paid for, such as the False Claims Act.

How to Handle It

The environment is evolving so rapidly that sector-wide best practices have not yet crystallized. However, Cliffe, Freeman, and Choi say there are practical steps contractors can take:

- Emphasize supply chain security in compliance programs and processes. Incorporating supply chain security into the existing compliance program requires participation by various parts of the company such as IT, trade compliance, procurement, human resources, and quality.
- Review contracts to fully understand what subcontractors must do and to strengthen contractual requirements.
- Apply greater vigilance when vetting, selecting, and monitoring subcontractors and suppliers.
- Strengthen review and reporting mechanisms to more effectively detect and report issues.
- Verify subcontractor performance via certification clauses or mandatory audits and develop corrective action plans where gaps are identified.
- Document more, rather than less, to be ready for government audits or inquiries.
- Train internal stakeholders to deal with existing requirements and to look out for new ones.
- Know what your competitors are doing and how your government customers and regulators respond.

Perhaps the most important thing, Cliffe says, is to adopt a mind-set that looks beyond mere compliance and into the long term. "The most successful contractors," she says, "will be those that can constantly look ahead, analyze what's going on, regroup as needed, and quickly adapt."

"We also anticipate increased supply chain-based activity from relators and whistleblowers, which should prompt more litigation." **Judy Choi**