GOVERNMENT CONTRACTS

BATTENING DOWN THE HATCHES ON CYBERSECURITY

Doing business with the U.S. government is about to get tougher as federal requirements for cybersecurity become stricter.

While the need to protect sensitive government information and technology isn't new, its importance in government contracting has historically—and understandably—been highest in the defense sector. The government's heightened focus on cybersecurity will become sharper in 2019, when the Trump administration is expected to finalize a new proposed clause in the Federal Acquisition Regulation (FAR) that essentially extends the application of stringent Department of Defense cybersecurity rules to non-defense contractors, as well.

The new regulation focuses on so-called controlled unclassified information (CUI), which is government information that is considered sensitive and requiring protection but that doesn't rise to the level of classified information. Common categories of CUI arising in government contracting include controlled technical information, export control information, privacy information (e.g., personal identifiers and health data), procurement and acquisition information, and proprietary business information.

For federal contractors, the message is clear: Cybersecurity is here to stay and will only become more critical if you want to work with government agencies.

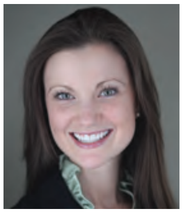
WHAT TO EXPECT: EMERGING TRENDS

The FAR clause's implications will likely extend beyond contractors, notes Evan Wolff, a Crowell & Moring partner and co-chair of the firm's Privacy & Cybersecurity Group, who formerly served as an advisor to the senior leadership at the Department of Homeland Security. "Cybersecurity concerns are an increasingly common and integral aspect of corporate existence," he says. "The application of defense-quality requirements to all government contractors will likely have a trickle-down effect on the private sector."

Wolff sees several trends emerging as the new rule percolates through the administrative process:

- **Continued tightening of government cybersecurity standards.** As a matter of national security, the government will insist that its vendors maintain adequate protection to secure their IT networks against cyberthreats. Companies will accordingly put more effort and resources into cybersecurity.
- **Extension through the supply chain.** The government's cybersecurity standards often apply to subcontractors as well as prime contractors, which likely will force many subcontractors to adequately protect their networks—an investment they may not be able to afford—or risk losing their government business. This scenario isn't unusual, says Kate Growley, a counsel in Crowell & Moring's Privacy & Cybersecurity and Government Contracts groups. "There are prime contractors that don't appreciate how government requirements can put real hardship on subcontractors," says Growley, "as well as subcontractors that don't know that prime contractors have to meet the requirements in the first place. If both want to succeed, they'll have to understand that cybersecurity is a shared responsibility."
- **Competitive differentiation.** Increasingly, companies will be evaluated by their level of, and commitment to, cybersecurity. Those that are cybersecure will have a significant competitive advantage over companies that aren't, whether as government contractors or more generally. They'll be seen as more desirable vendors, partners, acquirers, or targets.
- **Corporate lifecycle issue.** Cybersecurity will become more of a determinant of corporate survival, and not simply because its absence exposes companies to existential threats

" The application of defense-quality requirements to all government contractors will likely have a trickle-down effect on the private sector." *—Evan Wolff*



“Prime contractors should expect to deal with noncompliant subcontractors and be prepared to figure out a compliance workaround, which can be a difficult and complicated task.” —*Kate Growley*

such as hacking. Wolff notes, “We’re seeing more and more companies in M&A transactions analyzing the other party’s cybersecurity as a key criterion for making the deal. Over time, companies that aren’t cybersecure may find themselves standing still, or even going out of business, as their cyber-savvy competitors move forward.”

- **Cultural imperative.** Cybersecurity will transcend its initial status as a purely technological matter and rise in importance to become part of companies’ cultural fabric, much like teamwork, safety, and cost-consciousness. It’s already a board-level concern at many companies, a standing that should grow into mainstream practice.

CYBERSECURITY AS A TEAM SPORT

One approach to cybersecurity counseling that has proven to be effective emphasizes cultural reinforcement and the development of a corporate infrastructure. As Wolff puts it, “Companies should think of cybersecurity as a team sport. Ideally, all parts of the company, from the board to operations, sales, legal, administration—everyone, really—should collaborate to keep the organization safe.”

An exemplary infrastructure would include these elements:

- **Appointment of a chief information security officer**—distinct from an all-encompassing CIO or CTO—commits dedicated resources to cybersecurity and signals to employees, customers, competitors, and investors alike that the company considers cybersecurity a priority.
- **Vulnerability analyses** help companies identify their weakest links—the first step toward achieving cybersecurity.
- **Conducting incident simulations, developing an incident response plan, and creating an incident response team** intensify awareness of cyberattacks and condition the company to deal with them. Think of this as the electronic equivalent to fire preparedness.
- **Training policies and procedures** are vital to maintaining cybersecurity and keeping everyone on the same page.
- **Physical, technical, and administrative controls** ensure that the right protections are in place and working.
- **Cyber-specific auditing and reporting processes** create and track accountability.
- **Due diligence capability for M&A and other transactions** evaluates the cybersecurity of potential targets and partners—and can serve as a yardstick for whether the evaluating companies are current on best practices.
- **Anticipation and assessment of litigation risks** takes on heightened importance in the constantly changing cybersecurity environment.
- **The purchase of cyber insurance** is an under-the-radar option that could be particularly helpful for smaller businesses with limited resources.

“Organizations that can build a sound infrastructure position themselves not only to deal with cyberthreats, but also to achieve greater success,” Wolff says. “The time is coming when the cost of *not* being cybersecure will be higher than the cost of maintaining best practices. Companies won’t want to be caught holding the bag when that happens.”

GETTING CREATIVE TO GET THE CONTRACT

Cybersecurity doesn’t have to be an all-or-nothing proposition for government subcontractors. Sometimes a little creativity goes a long way.

This can be the case when there’s only one subcontractor available that can provide a specialized product or service needed to satisfy a contract. Crowell & Moring’s Kate Growley notes that such sole-source providers are often small and don’t meet the government’s cybersecurity requirements. “Prime contractors should expect to deal with noncompliant subcontractors and be prepared to figure out a compliance workaround, which can be a difficult and complicated task,” she says.

The problem typically boils down to how to safeguard confidential government information when the subcontractors lack the necessary network protections. Growley says that prime contractors should start by asking, do we even need to share the information with the subcontractors at all, and, if yes, do they need to store it electronically.

A straightforward, cost-effective solution can be for the subcontractor to use a third-party-managed service provider whose storage capabilities are already compliant. This isn’t always practical—which is where creativity comes in. In such instances, old-school use of paper copies can do the trick, as securing paper is usually much easier than securing a network. Another approach: have the prime contractor handle electronic storage and let the subcontractor view it on a secure portal or by visiting the facility.