wiley

NEWSLETTER

Hill Increasingly Focused on Cybersecurity Threats and Private Sector Responses: Looming Effects on Government Contractors

Winter 2012

Momentum is building in Washington to act on cybersecurity reform. Whether Government action is targeted or comprehensive, companies in various sectors and across the government contracting community are likely to face new regulation and oversight.

Many elements of proposed legislation center on the need to secure "critical infrastructure." While critical infrastructure's exact definition will most likely be determined at the agency level, the term is used colloquially to refer to infrastructure whose proper function is vital to the country's national security, economy or public heath and safety. Any definition likely will cover at least some systems and materials provided or serviced under government contracts.

New cybersecurity regulations could provide new opportunities for companies seeking government contracts-particularly those in the IT sector. And contractors should prepare to participate in the eventual regulatory proceedings at the Department of Homeland Security or other implementing agencies by evaluating their current cybersecurity plans and considering what burdens they can live with in the future.

Because private entities create and operate systems, equipment and infrastructure that could be subject to treatment as critical infrastructure, government contractors should pay attention to the proposals presently being considered.

Despite myriad hearings on cybersecurity over the past couple of years, momentum for significant legislation and possible impacts to industry has been increasing given the number of cyber attacks that

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Brandon J. Moss
Partner
202.719.7554
bmoss@wiley.law

have made headlines in recent months.

Last week, the Senate Committee for Homeland Security and Government Affairs (HSGAC) released its final draft of the Cybersecurity Act of 2012. Of particular importance for companies that contract with the Government, the bill would require the federal Government to develop a comprehensive acquisition risk management strategy and amend the current Federal Information Security Management Act. Additionally, legislation may direct the Office of Management and Budget to develop security requirements and best practices for all federal IT contracts.

The House has been active as well. Lawmakers have signaled support for a bill proposed by House Intelligence Chairman Mike Rogers (R-MI) to facilitate information sharing regarding cyberthreats between the private sector and the government. Though the House has not produced draft comprehensive legislation, a number of relevant committees have been engaged. For example, on February 8, 2012, the House Subcommittee on Communications and Technology held a hearing titled "Cybersecurity: Threats to Communications Networks and Private Sector Responses." The House Energy and Commerce Committee is said to be working on legislation and the House Homeland Security Subcommittee on Cybersecurity has advanced its bill, H.R. 3674, the PRECISE Act.

Eventual legislation is likely to include various provisions that could pose challenges or opportunities for government contractors.

For example, previous proposals indicate that some contractors may have to (1) comply with substantive obligations relating to the production, maintenance and operations of critical infrastructure; (2) make disclosures to the Government regarding information relating to security or potential or actual cyberattacks; (3) employ the services of third-party cybersecurity accreditors; (4) carry cyber liability insurance; (5) have overseas operations subject to additional, potentially conflicting, U.S. obligations; (6) and possibly comply with requests for emergency takings of critical infrastructure.

On the other hand, legislation could include beneficial provisions that: (1) limit civil liability; (2) preempt duplicative or contradicting state and local standards; (3) simplify and streamline existing regulations; (4) help industry freely communicate with the government regarding cyberthreats; and (5) limit strategic use of FOIA to access corporate documents.

These developments should put the private sector on notice that the government will be taking action. The Senate HSGAC Committee is holding hearings and the possibility exists that floor action could be expedited. Moreover, the Senate Armed Services and Commerce Committee Members may release a less comprehensive but potentially more vote-viable bill. With the various House Committees active on this issue, it is clear that there are a number of threats and opportunities on the Hill in cybersecurity. Thus, all government contractors should evaluate their polices and keep an eye on Washington as Congress continues to debate, and potentially enact, cybersecurity legislation.