wiley

NEWSLETTER

Cybersecurity Legislation and Its Impact on Government Contractors

Spring 2011

In FY 2010, federal agencies faced a 40 percent increase in cyber incidents compared to the number of incidents in FY 2009, according to Office of Management and Budget's (OMB's) FY 2010 Federal Information Security Management Act (FISMA) Report. Incidents include unauthorized access, denial of service and malicious code. The incidents reported for federal agencies do not capture the larger threat to the private sector, which owns over 80 percent of the information infrastructure in the United States.

The heightened threat level has substantially increased the likelihood of congressional action on some form of cybersecurity legislation this year. Members of Congress on both sides of the aisle recognize the significant cybersecurity threat that the U.S. government faces-particularly to the federal information technology infrastructure. One senior Senate staffer recently commented that members are "serious" and "bipartisan" on the issue. A draft comprehensive cybersecurity bill is currently with Senate Majority Leader Sen. Harry Reid for consideration, and congressional staff expect such a cybersecurity bill on the floor this summer.

The cybersecurity legislation currently under consideration will affect government contractors in a number of ways. First, such legislation will define who does what in the federal space and point toward future business opportunities in cybersecurity. Second, government contractors can expect such legislation to leverage federal buying power to promote cybersecurity through requirements for minimum security standards and supply chain risk management efforts. Third, government contractors can expect to see efforts to improve information sharing with the private sector and other stakeholders in the cybersecurity space. Fourth, critical infrastructure entities in sectors such as the defense industrial base and communications could be subject to performance-based regulations overseen by DHS.

In the last Congress, there were over 60 pieces of cybersecurity-related legislation, but few of these saw final action. This year, it appears that the Senate is taking the lead on comprehensive cybersecurity legislation, while the House is taking a more piecemeal approach. Senators Joe Leiberman (I-CT), Susan Collins (R-ME) and Thomas Carper (D-DE) have co-sponsored S.413, the Cybersecurity and Internet Freedom Act of 2011, which is becoming the centerpiece framing the debate on comprehensive cybersecurity legislation. The comprehensive Leiberman/Collins bill would codify current agency activities and expand certain agency authorities. However, as the sponsors of the bill made clear when it was introduced in February 2011, the bill does not provide for an Internet "kill switch." There were significant concerns during debate in the last

Congress that the prior Leiberman/Collins bill would allow the President to shut down the Internet.

There are provisions of S. 413 that will be of particular interest to the procurement community. For example, S.413 requires DHS to develop a Strategy for Federal Cybersecurity Supply Chain Management. The Strategy must be developed in consultation with the White House, other agency stakeholders, the Administrator for Federal Procurement Policy, Chief Information, Acquisition, and Financial Officers Councils and the private sector. The Strategy places particular emphasis on developing processes that:

- "Assess risks from potential suppliers providing critical components or services of the federal information infrastructure";
- "Manage the quality, configuration, and security of software, hardware, and systems of the Federal information infrastructure throughout the life cycle of the software, hardware, or system . . ."; and
- "Enhance developmental and operational test and evaluation capabilities, including software vulnerability detection methods and automated methods and tools that shall be integrated into acquisition policy practices by Federal agencies . . . "

The legislation also calls for the FAR Council to amend the FAR to implement the Strategy by directing that "all software and hardware purchased by the Federal Government shall comply with standards developed or be interoperable with automated tools approved by the National Institute of Standards and Technology." Finally, the Strategy must include a preference for the acquisition of commercial items.

Other key provisions of S.413 would:

- Establish an Office of Cyberspace Policy in the White House and a director who would have authority to review and make recommendations on agency budgets to address cybersecurity issues. This would codify the current White House Cybersecurity Coordinator position and clarify his authority.
- Establish a National Center for Cybersecurity and Communications within DHS, establish a director to oversee cybersecurity functions within DHS and clarify DHS cybersecurity authority. The bill would require some adjustments at DHS but is largely consistent with DHS efforts to consolidate certain cybersecurity functions in the National Cybersecurity and Communications Integration Center.
- Reform FISMA by shifting from a paper-based reporting effort to a real-time effort to secure federal information infrastructure. DHS would have authority to oversee the civilian agency efforts to secure the federal information infrastructure, approve agency information security plans and coordinate response incident efforts. Further, DHS could order that an agency be "isolated" from other Federal information infrastructure if the agency does not implement a risk-based plan to address vulnerabilities identified in operational evaluations. These provisions are consistent with July 2010 OMB guidance that effectively gave DHS the lead for FISMA activities.
- Require DHS to issue interim final regulations establishing risk-based security performance requirements to secure "covered critical infrastructure." DHS would designate an entity or asset as "covered critical infrastructure" with input from various stakeholders based on certain criteria; however, such designation could be appealed.

- Authorize the President to declare a national "cyber emergency" that would, in turn, authorize DHS to direct covered critical infrastructure to implement response plans and direct that emergency measures be taken. The bill also provides for certain liability protection for a covered entity's compliance with emergency measures.

While the Senate is expected to take a broader leadership effort on cybersecurity legislation, other stakeholders can be expected to play key roles. Key among these stakeholders is the White House, which was relatively silent on cybersecurity legislation in the last Congress. The White House has engaged in over a year-long inter-agency process to evaluate its position on cybersecurity legislation and is being pressed by the Congress to provide feedback. In the House, jurisdiction issues stymied cybersecurity progress in the last Congress, but in December 2010, Speaker John Boehner identified Vice Chairman of the Armed Services Committee Mac Thornberry as the point person in the House for Cybersecurity. Thus far, there has been little activity on cybersecurity in the House because much of the effort in the early part of this Congress has been focused on budget issues, but members remain engaged and interested in cybersecurity. If the Senate passes a bill, the House will be hard pressed not to consider it.

In sum, Government contractors should watch for cybersecurity legislation action this Summer because Congress appears poised to act on such legislation. This legislation will certainly impact business opportunities and the federal information technology acquisition process as Congress attempts to leverage the buying power of the federal government to improve cybersecurity. With agencies spending $12 billion, or 15 percent of the federal information technology budget, on cybersecurity in FY 2010, the stakes are high.