Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cybersecurity Reforms Likely As Contractor Support Grows

By **Dietrich Knauth**

Law360, New York (March 20, 2012, 6:42 PM ET) -- While several cybersecurity bills are competing for passage in Congress, the Cybersecurity Act of 2012, introduced by Sens. Joe Lieberman, I-Conn., and Susan Collins, R-Maine, and backed by the White House, has a broad base of industry, contractor and government support, and includes many provisions that are likely to make their way into any eventual reform, experts said.

The bill, and others like it, address several key aspects of cybersecurity reform, including creating a mechanism to safely share information on new and emerging threats, allowing the U.S. Department of Homeland Security more authority to monitor and combat cyber threats, and giving the government authority to require stricter electronic protection for infrastructure that is privately owned but important for national security, such as power grids.

Lawmakers on Capitol Hill have shown an intense interest in cybersecurity, but have not passed new legislation in the area since the 2002 Federal Information Security Management Act. Cyberthreats have grown steadily since then, with Secretary of Defense Leon Panetta repeatedly warning that the U.S. could face a digital Pearl Harbor unless it shores up its electronic defenses, and Joe Lieberman saying that a cyberattack could cause more destruction than the terrorist attacks of Sept. 11, 2001.

"If you're not scared by now, you're either dead or tougher than woodpecker lips," said David Bodenheimer, a partner in Crowell & Moring LLP's government contracts group.

Government contractors are doubly vulnerable to cyber threats, according to Elizabeth Ferrell, a partner in McKenna Long & Aldridge LLP's government contracts practice. Working with government information makes contractors attractive targets to hackers, and federal agencies often have enough leverage to force contractors to accept much of the financial risk associated with hacking attacks.

"All government contractors, whether they host systems for the government or provide other services, are kept up at night thinking about how disastrous a cyberattack on their company would be," Ferrell said.

Despite a long-standing consensus that U.S. data systems need better protection, lawmakers have not agreed on the best way to improve security. Just weeks after Lieberman and Collins introduced their bipartisan bill, Sen. John McCain, R-Ariz., led a Republican coalition in bringing up an alternative. Still, the Cybersecurity Act of 2012, which has bipartisan support; the backing of Senate Majority Leader Harry Reid, D-Nev., and the White House; and many provisions in common with McCain's bill, is a good place for contractors to look as they prepare for cyberlegislation.

"We need to do something, and while [the Cybersecurity Act] has some negatives, it at least has a framework that we can debate," Bodenheimer said.

The bill has the support of Secretary of Homeland Security Janet Napolitano, who said that the law would give her office the tools it needs to combat cyberthreats while "protecting privacy, confidentiality and civil liberties." And several companies, including contractor Northrop Grumman, have supported both the bill and the "open dialogue" between government and affected industry players.

"Northrop Grumman applauds Congress' commitment to strengthening our nation's cybersecurity posture," Chairman and Chief Executive Officer Wes Bush wrote in a letter to the bill's sponsors. "Northrop Grumman supports the enactment of cybersecurity legislation that ... [s]trengthens critical infrastructure protection and facilitates the sharing of threat information across the public and private sectors."

Among the reforms in the Cybersecurity Act, the one that is closest to a "no-brainer" is a section that would create federal information exchanges to facilitate sharing of information about cyberthreats, both by the government and industry, attorneys said.

"Information sharing is one of the linchpins of an effective cybersecurity defense," Bodenheimer said.

Under the current regulatory framework, which sets internal government security standards and practices, there's no real system in place for sharing information about new and emerging cyberthreats. Government bodies may not share information because it is nonpublic or classified, and companies may not share information because they are concerned about exposing themselves to further harm or litigation if they reveal their vulnerabilities, Ferrell said.

Proactively sharing threats "requires a lot of thought by somebody," Ferrell said. "We don't have enough resources for everybody to do it independently."

Both McCain's bill and the Cybersecurity Act include protection for companies that disclose the existence of threats, shielding them from liability to some extent and protecting such disclosures from Freedom of Information Act requests.

And both McCain's bill and the Lieberman-Collins bill address the government's need to protect critical infrastructure that could be targeted by cyber attacks — including the power grid, communications systems and water supply, for example — though they differ in approach. In the biggest divergence between the bills, McCain's proposal would essentially allow the industry to regulate itself, while the Cybersecurity Act of 2012 would allow DHS to designate certain industries as "critical infrastructure" and regulate their cyberdefenses.

McCain argued in a congressional hearing that the move would turn DHS into a "regulatory Leviathan" that would strangle businesses with burdensome regulations, but others saw government intervention as a necessary step to shore up weaknesses that could affect national defense.

Steptoe & Johnson LLP partner Stewart Baker, a former assistant secretary for policy at DHS who testified in favor of the bill, said it would be a mistake to trust the private sector to beef up security on its own, as did Bodenheimer.

“The current industry practices are failing,” Bodenheimer said.

Lieberman has said that he welcomes a dialogue with supporters of McCain's bill, to address the need for reform.
Whether or not the particular provisions are enacted, experts agreed that current law, which sets some standards for government data while relying on industry players to police themselves, needs to change.

And even after legislation fixes some of the weaknesses in the nation's cyberdefenses, contractors and the government will need to remain constantly vigilant to stay one step ahead of rapidly evolving threats: no set of standards or best practices will ever keep systems safe for long, according to Ferrell.

"Cybersecurity systems can't be static," Ferrell said. "They have to be flexible and have to change as threats change."

--Editing by Cara Salvatore.