

## Can Cybersecurity Legislation Overcome Partisan Divide?

*Law360, New York (March 19, 2012, 2:16 PM ET)* -- In the fall of 2011, many observers thought substantial cybersecurity legislation had a good chance of being enacted in the 2012 congressional session. Both President Obama and Senate Majority Leader Harry Reid, D-Nev., publicly identified cybersecurity as a top legislative priority for the new congressional session.

Five months later, the prospects for federal cybersecurity legislation seem much less certain. Rival Democratic and Republican bills have been introduced in the Senate, and several proposals are under consideration in the House. Still, both Senate bills and their House counterparts share a number of elements in common. On March 13, Sen. Joe Lieberman, I-Conn., stated he would seek to meet with Sen. John McCain, R-Ariz., to see if they could bridge the differences between their bills. If sweeping cybersecurity legislation seems unlikely to be enacted this year, a more modest package of cybersecurity initiatives may yet emerge from Congress.



### Senate Proposals

After months of negotiations and a series of classified briefings on cyber threats by members of the administration's national security team, Sens. Joe Lieberman, Susan Collins, R-Maine, Dianne Feinstein, D-Calif., and Jay Rockefeller, D-W. Va., introduced their omnibus Cybersecurity Act of 2012 (S. 2105) on Feb. 14, 2012. The bill would:

- authorize the U.S. Department of Homeland Security to identify and establish cybersecurity performance standards for "covered critical infrastructure," such as important energy, financial, telecommunications and transportation systems or assets (Title I);
- clarify the authority of owners of information systems to monitor and undertake "countermeasures" on their own systems and create institutions and legal incentives for the sharing of cyber threat and response information among businesses and between businesses and the federal government (Title VII); and
- strengthen the ability of the federal government to protect its own networks and centralize enhanced authority in DHS (Titles II and III).

The bill would not establish a federal data breach notification standard.

At the hearing held on the bill two days later before the Senate Homeland Security and Government Affairs Committee (chaired by Lieberman, with Collins as ranking member), it quickly became clear that leading Senate Republicans would not back the bill, particularly because of its inclusion of authority for new federal cybersecurity requirements for critical infrastructure.

Within two weeks, Sens. John McCain, Kay Bailey Hutchison, R-Texas, Saxby Chambliss, R-Ga., Charles Grassley, R-Iowa, Lisa Murkowski, R-Ark., Dan Coats, R-Ind., and Ron Johnson, R-Wis., introduced their alternative bill, the Secure IT Act of 2012 (S. 2012). Like the Cybersecurity Act, the Secure IT Act contains titles addressing uncertainty regarding laws relating to companies' monitoring of their own networks and to information-sharing within the private sector and between the private sector and the government (Title I) and providing for enhanced authority for DHS to coordinate information security policy for federal networks (Title II).

## Critical Infrastructure

The biggest difference between the two Senate bills is the omission from the Republican Secure IT Act of authorization for federal cybersecurity standards for critical infrastructure systems. Under the Lieberman-Collins bill, by contrast, DHS would be required to issue rules, within one year, establishing sector-specific cybersecurity performance requirements (§ 104); owners (not operators) of covered systems or assets would have to certify compliance annually or get third-party assessments of their compliance, and establish response plans and report on cybersecurity incidents. (§ 105).

The DHS rules would be issued following a two-step process in which, after consultation with other federal agencies and private-sector actors, DHS would have 90 days to assess the degree of cyber risks in different economic sectors containing critical infrastructure and establish a priority list of sectors requiring most urgent attention (§ 102) and would then be required, through a consultative process with other agencies and private-sector stakeholders, to designate "covered critical infrastructure" at the system and asset level (§ 103(a)).

Systems or assets could be designated as "covered critical infrastructure" only if damage or unauthorized access to that system or asset could reasonably result in:

- (i) the interruption of life-sustaining services, including energy, water, transportation, emergency services, or food, sufficient to cause —
    - (I) a mass casualty event that includes an extraordinary number of fatalities; or
    - (II) mass evacuations with a prolonged absence;
  - (ii) catastrophic economic damage to the United States including —
    - (I) failure or substantial disruption of a United States financial market;
    - (II) incapacitation or sustained disruption of a transportation system; or
    - (III) other systemic, long-term damage to the United States economy; or
  - (iii) severe degradation of national security or national security capabilities, including intelligence and defense functions
- § 103(b).

The bill twice expressly provides that the new requirements could not directly specify how particular hardware or software should run or require inclusion or exclusion of particular IT products (§§ 103(b); 104). The new federal standards would preempt state or local laws or rules "that expressly require[] comparable cybersecurity practices to protect covered critical infrastructure" (§ 111), and compliance with the standards would protect owners of covered critical infrastructure from punitive damages in "any civil action for damages directly caused by an incident related to a cyber risk identified, so long as they are in compliance with the various cybersecurity requirements established under the Act" (§ 105(e)).

Owners of assets or systems designated as "covered critical infrastructure" would have a number of ways to avoid the new mandates:

- DHS would be required to establish a process by which an owner of a covered system or asset could show its cybersecurity was good enough to warrant exemption from the new requirements (§ 105)

- DHS could determine that no new regulations are required if existing sector-specific regulations set sufficiently high requirements (§ 104(c))
- The President could exempt parts of covered critical infrastructure if he determined that a sector-specific agency's requirements and enforcement mechanisms were sufficient to mitigate cyber risks (§ 104(f))
- The only provision directly addressing critical infrastructure in the Secure IT Act, by contrast, is a section (§ 305) establishing enhanced criminal penalties for damaging a computer that manages or controls critical infrastructure systems.

## **Monitoring and Information-Sharing**

When it comes to monitoring and information-sharing, the Senate bills' common elements are probably greater than their differences. Both would authorize private entities to monitor their own networks and to employ "countermeasures" to cyber threats. Both would provide specific authorities for voluntary sharing of cyber threat information among private entities and between private entities and the government.

Among the notable differences between the bills:

- The Cybersecurity Act would create federal "cybersecurity exchanges," with DHS at the top, whereas the Secure IT Act would designate existing government organizations as "cybersecurity centers," and many of those organizations would be in the military and intelligence agencies
- Under the Cybersecurity Act, cybersecurity exchanges handling private information would be subject to privacy and civil liberties guidelines and would be permitted to retain or use the information only for information security purposes; federal cybersecurity exchanges would be permitted to share information relating to criminal activity with law enforcement with approval of the Attorney General (§ 704)
- Under the Secure IT Act, federal contractors providing electronic communications services, remote computing services, or cybersecurity services to federal agencies would be required to share cyber threat information related to the contract work with the agency for which they were a contractor (§102(b))
- Under the Secure IT Act, the Director of National Intelligence and the Secretary of Defense would be required to establish procedures to facilitate the sharing of classified cyber threat information with appropriately cleared entities outside the government (§ 103)

One of the leading cybersecurity bills in the House, H.R. 3523, also focuses on information sharing. Sponsored by Reps. Mike Rogers, R-Mich., and C.A. "Dutch" Ruppersberger, R-Md., H.R. 3523 would authorize private entities to monitor their own networks for cybersecurity threats (though not expressly authorize countermeasures) and would provide legal encouragement for information sharing in the private sector (but not establish specific federal cybersecurity exchanges). Approved by the House Intelligence Committee by a 17-1 vote in December 2011, the bill appears to have considerable bipartisan support.

## **Federal Networks**

Both Senate bills include nearly identical titles providing for enhanced and more centralized authority to protect the federal government's own networks, with DHS becoming the lead agency for federal cybersecurity requirements and planning.

## Prospects

The principal point of contention between Democrats and Republicans in the Senate appears to be over inclusion of critical infrastructure requirements. The administration and Senate Democratic leaders continue to press for those requirements on national security grounds — for example, sponsoring an exercise showing a mock cyber attack on the electric grid on March 7 — but with Sen. Lieberman already suggesting he is interested in finding common ground with Sen. McCain, a possible compromise bill featuring at least a title on monitoring and information-sharing and a title on improving protection of federal networks may be the more likely outcome.

Bill hyperlinks:

<http://www.gpo.gov/fdsys/pkg/BILLS-112s2105pcs/pdf/BILLS-112s2105pcs.pdf>

<http://www.gpo.gov/fdsys/pkg/BILLS-112s2151is/pdf/BILLS-112s2151is.pdf>

<http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523ih/pdf/BILLS-112hr3523ih.pdf>

--By Jonathan G. Cedarbaum, Benjamin A. Powell and Jason C. Chipman, WilmerHale LLP

Jonathan Cedarbaum and Benjamin Powell are partners, and Jason Chipman is a counsel, in WilmerHale's Washington, D.C., office.

The opinions expressed are those of the authors and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] A fuller analysis of the bill can be found here:

<http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=10038>.

[2] A video of the hearing and witness statements can found here:

<http://www.hsgac.senate.gov/hearings/securing-americas-future-the-cybersecurity-act-of-2012>.

[3] For a broader overview of likely legal developments related to cybersecurity, see:

<http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=10038>.

All Content © 2003-2012, Portfolio Media, Inc.