Written by **Raven Clabough** on July 25, 2012

Senate to Consider Cybersecurity Act of 2012

The U.S. Senate is preparing to take up the Cybersecurity Act of 2012, which critics contend does not have the significant teeth necessary to prevent a massive cyberattack against the United States. Though the bill underwent a number of changes to appease those who voiced privacy concerns, it remains controversial.

According to the bill's sponsors, Senators Joe Lieberman (I-Conn.) and Susan Collins (R-Maine), the bill's focus is on protecting the electric grid, water systems, financial networks and transportation systems from the threat of cyber attacks.

But the bill in its original form posed too many privacy concerns and faced opposition from those on the right and the left.

On July 19, Senator Lieberman unveiled a newer, revised version of the bill, that, despite revision, remains controversial.

The bill's sponsors made some concessions and revised components of the original bill that drew significant criticism, including the provision to assign the Department of Homeland Security the role of creating mandatory cyber security standards for infrastructure industries.

The newer version of the bill does not include language for "mandatory, regulatory sections," but still requires a creation of industry "best practice" standards for the purposes of protecting critical infrastructure. Rather than making the adoption of those standards mandatory, moreover, the owners of the critical infrastructure may adopt "voluntary" standards. The bill offers incentives to adopt those standards, such as liability protection, and access to threat information.

But as noted by Heritage.org, that approach poses too many problems:

> The government should not be in the position of denying its threat information to critical infrastructure owners who choose not to adopt the voluntary standards, likely for justifiable business reasons. If the infrastructure in question is truly "critical," it is in America's collective interest to protect it as much as possible.

Likewise, the liability protection offered is not significant enough to incentivize owners of critical infrastructure because companies that adopt the standards could still be sued for consequential damages. The liability protection offered only covers punitive damages.

Heritage.org notes that the voluntary standards "would stifle innovation and likely be obsolete by the time they are written." It explains, "No thoughtful investor will invest in a product that might not be one of the standard-approved methods of providing cybersecurity, even if it might be a better one."

And most notably, voluntary standard systems can too easily become mandatory standard systems. Senator Lieberman has already stated that if enough industries do not adopt the standards, Congress

will mandate that they do so.

Additionally, the sponsors made revisions to the original bill based on concerns that the military and national security agencies had too much direct involvement.

Lieberman explains, "We wanted to set up a system where, to the greatest extent we possibly could, we guarantee people that their privacy would not be compromised, their personal privacy, in pursuit of making the country safer from cyber-attack. We've done that."

Still, even with the changes, many companies in the business sector remain opposed to the bill.

"While this sounds appealing on its face, a government-administered program would shift during the implementation phase from being standards based and flexible in concept to being overly prescriptive in practice," Ann M. Beauchesne, the Chamber of Commerce's vice president of national security and emergency preparedness, said in a statement.

And regardless of the changes, any bill that allows data to be shared with national security and intelligence agencies is likely to provoke privacy concerns.

Others believe the bill has been altered too much so that it does not offer any real protection against cyber attacks.

Senators "have two weeks to put some teeth back in," James A. Lewis of the Center for Strategic and International Studies said in an interview. "Then they need to make it an up-or-down vote. Are you for national security? Or does that come second?"

If passed in the Senate, it would still need to be reconciled with a House bill that does not include any mention of standards.

President Obama has threatened to veto a cyber security bill that violates privacy protections, but has publically articulated his support for the bill in an opinion piece that he released last week, wherein he said that "the cyber threat to our nation is one of the most serious economic and national security challenges we face."

"On balance, we think that voluntary standards will still enable us to make meaningful improvements in cybersecurity," the White House's cybersecurity coordinator, Michael Daniel, said in an interview Tuesday. He conceded that the idea of mandatory standards was "legislatively almost impossible" right now, but "that's the ultimate goal."

Senator Lieberman has resorted to fear-provoking rhetoric to advocate for the bill's immediate passage:

> "The threat is extremely dire," Lieberman said. "I am literally worried that an attack could be imminent. We know that both states, countries like China, Russia and Iran are constantly probing our cyber networks, both government and private, and both civilian and defense.

"We know that countries and terrorist groups and organized crime groups are constantly trying to steal industrial secrets form American companies that they've invested millions in, sometimes billions in, to basically get it for nothing and then create those industries and jobs over in other countries."

Citing remarks made by Secretary of Defense Leon Panetta and National Security Agency head General Keith Alexander on the imminence of a cyber attack and the destruction it would cause, Lieberman said, "We're very vulnerable to attack and some of the private owners of critical cyber infrastructure, like the electric grid or the financial system, banking systems, transportation, water."

"Some of them are doing a pretty good job at defending their cyberspace, but some are not, and the main aim of this bill is to make sure that the private owners — 85 percent of our infrastructure … are taking steps to defend the cyberspace they own because that may well represent defense of our country."

Meanwhile, Republicans have threatened to delay consideration on the cyber security bill until the Senate takes up legislation on defense authorization.

Senate Majority Leader Harry Reid responded to such a threat by asserting, "Failing to act on cyber security legislation not only puts our national security at risk," but also "recklessly endangers members of our armed forces and missions around the world."

Photo: Sen. Susan Collins (R-Maine) the ranking member of the Senate Homeland Security Committee, right, and the committee's Chairman Sen. Joseph Lieberman (I-Conn.) during a news conference on July 24, 2012 to announce that the Senate will take up the Cybersecurity Act of 2012 later this week: AP Images