eWEEK.COM SECURITY

Bill Would Grant President Unprecedented Cyber-security Powers

By Roy Mark 2009-04-02

The Cybersecurity Act of 2009 introduced in the Senate would allow the president to shut down private Internet networks. The legislation also calls for the government to have the authority to demand security data from private networks without regard to any provision of law, regulation, rule or policy restricting such access.

The headlines were all about creating a national cyber-security czar reporting directly to the president, but the Cybersecurity Act of 2009 introduced April 1 in the U.S. Senate would also give the president unprecedented authority over private-sector internet services, applications and software.

According to the bill's language, the president would have broad authority to designate various private networks as a "critical infrastructure system or network" and, with no other review, "may declare a cyber-security emergency and order the limitation or shutdown of internet traffic to and from" the designated the private-sector system or network.

The 51-page bill does not define what private sector networks would be considered critical to the nation's security, but the Center for Democracy and Technology fears it could include communications networks in addition to the more traditional security concerns over the financial and transportation networks and the electrical grid.

"I'd be very surprised if it doesn't include communications systems, which are certainly critical infrastructure," CDT General Counsel Greg Nojeim told eWEEK. "The president would decide not only what is critical infrastructure but also what is an emergency."

The bill would also impose mandates for designated private networks and systems, including standardized security software, testing, licensing and certification of cyber-security professionals.

"Requiring firms to get government approval for new software would hamper innovation and would have a negative effect on security," Nojeim said. "If everyone builds to the same standard and the bad guys know those standards it makes it easier for the bad guys."

The legislation also calls for a public-private clearinghouse for cyber-threats and vulnerability information under Department of Commerce authority. The Secretary of Commerce would have the authority to access "all relevant data concerning such networks without regard to any provision of law, regulation, rule or policy restricting such access."

In another section of the bill, though, the president is required to report to Congress on the feasibility of an identity management and authentication program "with appropriate civil liberties and privacy protections."

Nojeim complained the bill is "not only vague but also broad. Its very broad language is intended to confer broad powers." Nojeim also speculated that the bill's vague language and authority may prove to be powerful incentive for the private sector to improve its cyber-security measures.

"The bill will encourage private-sector solutions to make the more troubling sections of the bill unnecessary," he said.

According to a number of media reports, the bill was crafted with the cooperation of the White House. The legislation aims to create a fully integrated, coordinated public-private partnership on cyber-security in addition to pushing for innovation and creativity in cyber-security solutions.

“We must protect our critical infrastructure at all costs—from our water to our electricity, to banking, traffic lights and electronic health records—the list goes on,” Sen. Jay Rockefeller (D-W.Va.), bill co-sponsor, said in a statement. “It’s an understatement to say that cyber-security is one of the most important issues we face; the increasingly connected nature of our lives only amplifies our vulnerability to cyber-attacks and we must act now.”

Fellow co-sponsor Sen. Olympia Snowe (R-Maine) added, “America’s vulnerability to massive cyber-crime, global cyber-espionage and cyber-attacks has emerged as one of the most urgent national security problems facing our country today. Importantly, this legislation loosely parallels the recommendations in the CSIS [Center for Strategic and International Studies] blue-ribbon panel report to President Obama and has been embraced by a number of industry and government thought leaders.”

The CDT’s Nojeim stressed that are a “number of good things in the bill,” including creation of a cyber-security czar, scholarships for cyber-security programs and collaborations between the government and the private sector. While urging Congress to change the bill, he argued that the “problematic provisions shouldn’t crowd out the beneficial provisions of the bill.”