

White House cyber adviser--more questions than answers

by [Stephanie Condon](#)

Font size

Print

E-mail

Share

 [Yahoo! Buzz](#)

The comprehensive [cybersecurity legislation](#) currently in development in the Senate aims to bring high-level government attention to the serious problem of cybersecurity by giving one White House official oversight of critical network infrastructure.

Yet the proposal in the draft legislation to give the national cybersecurity adviser the ability to disconnect federal or "critical" networks under threat of cyberattack may create more uncertainties than solutions, at least initially, cybersecurity experts warn.

Determining which networks are "critical" would be the first step to achieving security. A summary of the draft bill obtained by CNET News acknowledges the large swath of critical infrastructure that resides in the private sector-- banking, utilities, auto traffic control, and telecommunications.



Those networks all have different risk tolerances and means of mitigating risk--giving one person authority to disconnect any of them from the Internet would require a strong understanding of an overwhelming number of different systems.

"The irony is people keep on asking for somebody in charge who has this God's-eye view of what's going on in a purposefully decentralized system," said Bob Giesler, vice president for cyber programs at Science Applications International Corporation (SAIC). "This permeates the whole (cybersecurity) debate, which is what can the government do for us. I think you'll find at the end of Melissa Hathaway's 60-day (cybersecurity) review that industry will come back and say the best thing they can do is share the data so we can be better risk managers," rather than manage risk themselves.

In February, President Obama selected former Booz Allen consultant Melissa Hathaway, who also worked for the director of national intelligence in the Bush administration, to conduct a [review of](#)

federal cybersecurity activities.

Cutting off critical networks could have any number of impacts on consumers, depending on what services were disconnected, said Liesyl Franz, vice president for information security and global public policy at the trade organization TechAmerica. For instance, banks may stop distributing money through ATMs, government agencies may not be able to distribute services like food stamps or drivers' licenses, or financial institutions could stop trading.

However, "the best case scenario in this situation doesn't mean just (disconnecting networks) without collaboration," Franz said.

"The owners and operators themselves would be in a better position to say when they should disconnect networks," she said. "I would bet none of them would say the government should do it."

Rather than simply having an authoritative figure dictate when a network should shut down, she said, it would make more sense to establish a series of steps the public and private sectors could enact together in the face of a threat, based on the threat level.

Determining what threats merit significant action would be another challenge, given that networks of all kinds constantly face cyberattacks.

"Everybody is under attack, at some level, all the time," said Marjory Blumenthal, associate provost for academic affairs at Georgetown University and the founding executive director of the Computer Science and Telecommunications Board. Blumenthal was part of a commission that produced a report last year to advise the president on cybersecurity issues.

The lessons of history

The questions of which networks the federal government should oversee and what qualifies as sufficient protection are not without precedent. The Computer Security Act of 1987, for instance, aimed to improve the security and privacy of sensitive information in federal computer systems. It was initially unclear, however, whether the law should be applied to networks belonging to federal contractors.

Similarly, the National Communications System was established in the 1960s to coordinate operators on matters of national security. The scope of the office's jurisdiction has had to evolve, however, as service providers expanded to include groups like cable providers and Internet service providers.

This history may help government officials answer some of their

current questions and coordinate public-private partnerships, Blumenthal said.

"Because of the history of those bodies, there should be ways to leverage communication with at least the big networks," she said.

The history of federal network management may also explain why the drafters of the bill would want to put the authority to disconnect networks into the hands of a single individual, said Giesler. The military has managed a robust network that is constantly under attack. Yet because the network serves a limited number of users on a single domain, a military commander can make the decision to disconnect the network with a strong understanding of the consequences.

"The concept of governmental authority making that risk-gain assessment which could impact privately owned equities needs to be thoroughly discussed with the public," Giesler said. "It is a decision that should not be taken lightly."

Congress should also take the opportunity to collaborate with the private sector-- an opportunity largely enhanced by Hathaway's ongoing cybersecurity review, Franz said.

"We feel now there is an opportunity to share," she said. "There's been more galvanization of effort (in the last 30 days) than ever before."

Franz stressed that if a national cybersecurity adviser is indeed appointed, that person should have experience working with the private sector so that he or she can effectively maintain that public-private partnership.

Given the open questions of what networks should be deemed "critical" and when they may need to be shut down, "whoever is in the decision-making position is someone you hope is well-informed," Blumenthal said.

"You need somebody who understands the nature of systems--the way they interconnect, the different operating cultures," she said.

She said it may be premature to give a national adviser the authority to shut down networks, "but the devil is in the details."

"The irony is people keep on asking for somebody in charge who has this God's-eye view of what's going on in a purposefully decentralized system."

--Bob Giesler, VP for cyber programs, SAIC



Stephanie Condon is a staff writer for CNET News focused on the intersection of technology and politics. She is based in Washington, D.C. [E-mail Stephanie.](#)

Topics: [Regulation](#)

Tags: [cybersecurity](#)

Share: [Digg](#) [Del.icio.us](#) [Reddit](#)  [Yahoo! Buzz](#)

Related

From CNET

[Cybersecurity review is putting emphasis on privacy](#)

[Former FBI chief: NSA can't run cybersecurity alone](#)

[House politicians search for DHS cybersecurity fix](#)

From around the web

[Cybersecurity director resigns amid turf...](#)
AOL News

[Cyber director resigns amid federal turf...](#)
AOL News - Politics

[More related posts](#) powered by

 [Sphere](#)