

## Independent commission plans second report on cybersecurity requirements

By Jill R. Aitoro 07/24/09

The commission that provided the Obama administration with widely lauded recommendations for cybersecurity policies will develop recommendations for how the government can address possible issues such as privacy protection that could hinder the implementation of a plan to protect federal computer networks, commission members and industry representatives said on Thursday.

The Commission on Cybersecurity for the 44th Presidency submitted **25 recommendations** to the White House in December for improving protection of federal networks, many of which were included in the White House's cybersecurity plan **announced** May 29.

The commission, which was created by the Center for Strategic and International Studies in October 2007, plans to develop a second set of recommendations by the end of the year to guide implementation of the cybersecurity plan, the commission's four co-chairs told the press and Hill representatives.

"The first report was about the core conceptual problems, but there are foundational problems that if not resolved, make [success] difficult, even if you have the right policy framework," said Scott Charney, corporate vice president for Trustworthy Computing at Microsoft and a co-chairman of the commission. The other co-chairmen include Reps. Jim Langevin, D-R.I., and Michael McCaul, R-Texas; and retired Lt. Gen. Harry Raduege Jr.

He said an example of a foundational challenge would be the ability for government and industry to identify the source of a cyberattack without compromising the public's right to anonymity on the Internet.

"If you can't deal with the attribution problem, the policy choices become harder," Charney said. "The goal of this next phase is to look at those kinds of foundation problems, which are key to fixing the broader problems, and make concrete recommendations to the administration on how to address them."

The list of topics that will be included in the report is not complete. The commission will hold a full-day meeting on Friday to discuss the items members feel are most important to address, including privacy, civil liberties and engagement of international allies in implementing cybersecurity policy.

While the commission will discuss agencies' roles and responsibilities for implementing cybersecurity policies as they relate to specific recommendations, "to some extent, it would be inappropriate for the commission to micromanage the executive branch," Charney said.

He said a nonmilitary organization, specifically the Homeland Security Department, would be most appropriate to ensure the security of civilian and military networks. Charney and the other co-chairs reiterated their **recommendation** that the coordination of cybersecurity occur in the White House.

The report also will not directly address legal issues that could hamper government and industry partnerships, such as which organizations are accountable for cyberattacks and possible violations of antitrust laws from companies sharing information. The commission plans to leave those issues and regulations to Congress.

"We advocated in our initial report for a more operational public-private partnership," Charney said. "But the minute you talk about the government and private sector, issues arise [concerning] roles and responsibility and accountability. To the extent that those issues touch on the recommendations, we'll address them, but not as a separate topic. [Without] factual scenarios, the questions are too abstract."

A key requirement for implementing the recommendations is the appointment of a White House cyber adviser. Charney is **among the names** that have circulated as possible candidates. The administration has not confirmed who will fill the post.

"The [next] extremely important step is selecting a cyber coordinator," Langevin said. "The administration clearly understands the severity of the threat, but it remains unclear exactly how much access and authority this person will have."

He said the House Cybersecurity Caucus, which was formed in January to provide a forum for members representing different committees to discuss cybersecurity challenges, plans to invite the newly appointed cyber adviser to talk to the group.

Langevin also said he planned to introduce amendments to the Intelligence Authorization Act and the National Defense Authorization Act that would require a study to be conducted on retention of the cyber workforce, following a report released by Booz Allen Hamilton that showed critical shortages in skilled workers.

"Everything that's going on is moving so fast," said McCaul, pointing to the **recent cyberattack** that caused some agency Web sites to crash. "[The intent] was malicious, clear and specific to shut down. That's the kind of act I'm most concerned with [because] just about everything is tied to computer networks."

---

**COMMENT ON THIS ARTICLE IN THE FORUM**

---

---

© 2009 BY NATIONAL JOURNAL GROUP, INC. ALL RIGHTS RESERVED