



## Chertoff urges caution on potential of new cybersecurity laws

By [Ben Bain](#)

Published on October 8, 2008

Policy-makers and Congress should “proceed in a measured way” as they consider passing new laws or granting new authorities aimed at improving cybersecurity, the head of the Homeland Security Department said Wednesday.

DHS Secretary Michael Chertoff said he believes government has sufficient authority under current law to protect government and military assets. He also said that when working with the private sector on cybersecurity the government should “make sure we are invited in rather than pushing our way in.”

DHS plays a prominent role in the government’s multiyear, multibillion-dollar national cybersecurity initiative, which the administration launched earlier this year. The department is responsible for securing the .gov domain and is heading up efforts to work with private industry on the task. Meanwhile, the Defense Department is tasked with protecting the .mil domain and the Intelligence Community is responsible for its domain.

DHS’ new National Cybersecurity Center (NCSC) will bring together officials from DOD, DHS, the Office of the Director of National Intelligence and the Justice Department physically and virtually to coordinate operational efforts.

“The [National] Cybersecurity Center, when it’s fully operational, will be the operational forum or meeting ground where the various people...will come together and I think that’s going to be efficient,” Chertoff told reporters and bloggers today.

However, a panel of experts convened by the Center for Strategic and International Studies has criticized the government’s cybersecurity efforts as plagued with problems, including overlapping missions, poor coordination and a lack of a strategic focus (read [FCW’s story](#)).

The Cyber Commission on Cyber Security, which in September issued preliminary recommendations on how the next president should handle cybersecurity, pointed out that the most dangerous threats now come from foreign military and intelligence services and terrorist organizations. Only the White House, not DHS, has sufficient authority to oversee the government’s response to those threats.

The panel recommends that the White House foster a more collaborative approach to cybersecurity, taking advantage of the Internet and social networking technology to enable different agencies to work together.

Chertoff said the new NCSC was about “de-confliction” rather than command and control. He likened it to the different government participants working out who was going to try and catch a fly ball in baseball game. “In other words you got it, you got it, you got it — but not a command and control mechanism. Once you have it you execute under your orders.”

He also said that although NCSC will help different participants, with their different legal authorities, coordinate their responses to incidents, the White House will still coordinate the development of interagency policies.

“I think the report kind of looks at things as they maybe were a year or so ago,” Chertoff said when asked about the CSIS commission’s preliminary findings.

The commission recommended that the next administration and Congress work together to revise cyber crime investigative authorities, the Clinger-Cohen Act and the Federal Information Security Management Act.

The panelists also said that more regulations might be necessary to ensure the security of critical cyber infrastructure controlled by the private sector. But a command and control approach does not work with industry, they said. Instead, the government needs to foster a stronger public-private partnership.

Sponsored By



Chertoff also said he believed the private sector's engagement with the government on cybersecurity should be voluntary.

"I would not want to mandate our blocking mechanisms on the private sector," he said. "I would want the private sector to say...we want to have stuff that comes to our sensitive control systems go through a blocking system and help us construct that."

Chertoff said the government might determine later that new authorities and laws are needed. However, he said the government should be careful before increasing its intrusion in the public Internet.

"The Internet more than any other place has a distinctive culture that you don't want to break in order to protect, so my suggestion has been we proceed in a voluntary way, we proceed in a 21st century kind of collaborative way," he said.

© 1996-2008 1105 Media, Inc. All Rights Reserved.