



Government Needs To Get Its Cybersecurity In Gear, Experts Tell Congress

Security industry leaders agree that White House should lead revamped cybersecurity effort

By Tim Wilson, [DarkReading](#)

March 10, 2009

URL: <http://www.darkreading.com/story/showArticle.jhtml?articleID=215801683>

Some of the nation's top cybersecurity experts today told a congressional subcommittee that the United States isn't ready for a major online attack, and called on the White House and the rest of the federal government to get their acts together.

In a hearing held by the House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, four top IT security officials expressed concern about the government's slow movement in developing a defense for its own agencies and for the nation's critical infrastructure. All four said the White House should lead the effort with the creation of a civilian agency dedicated to cyberdefense.

"We need to face the fact that we are already dealing with cyberwar, both from criminal elements and from hostile governments," said Dave Powner, director of IT management issues at the Government Accountability Office. "We're constantly under attack."

"We're facing the same sort of attack we faced on 9/11, only on a virtual level," said Amit Yoram, CEO of NetWitness and a former White House cybersecurity official. "And without the right defenses, we'll be just as vulnerable."

The experts said that the White House should lead the effort to swiftly build up the nation's defenses against cyberattack. Jim Lewis, project director at the Center for Strategic and International Studies, said the White House is the only part of the government that has the budget and power to drive the initiative, and that only the president can make the decision as to when a cyberattack constitutes an act of war.

Mary Ann Davidson, CSO at Oracle, called on the federal government to develop an analog to the [target="new">Monroe Doctrine](#) that would clearly establish a U.S. "cyberturf" and a commitment to defend it with both offensive and defensive cyberweapons.

All of the experts, as well as some members of the subcommittee, expressed concern that the National Security Agency should be given the primary authority over U.S. cybersecurity initiatives. "Intelligence-gathering efforts often work at cross purposes with agencies that are developing defensive strategies," Yoran said.

Rod Beckstrom, the former director of the National Cybersecurity Center who [resigned last week in a turf battle with the NSA](#), was present at the hearing, but did not speak.

The White House is currently conducting a 60-day review of the cybersecurity situation; the review is expected to result in organizational recommendations for the Obama administration. The GAO has not yet met with the review committee, but Powner said his organization is recommending the formation of a White

House office responsible for cybersecurity. The GAO also is recommending the creation of a "board of directors" to monitor cybersecurity initiatives and an "accountable" cyberorganization that will speed the development of online defenses.

The members of the congressional subcommittee said they had many more questions for the experts, but they generally favored the recommendations made by the experts.

"The cybersecurity effort has been plagued by ineffective leadership," said Bennie Thompson, chairman of the subcommittee. "We were optimistic about the capabilities of Rod Beckstrom, but it became clear that he did not have experience in working miracles. He did not have the budget or the authority to get the job done. This committee believes, as he does, that there should be a civilian agency that interfaces with, but is not controlled by, the NSA."

Have a comment on this story? Please click [Discuss](#)'below. If you'd like to contact Dark Reading's editors directly, [send us a message](#)

&P&L W&K&W II I I I I I &0.310 H&C&V / &