

[House Panel Worries That Obama Cybersecurity Plan Could Open Door to Abuse](#)

(National Journal – May 25, 2011)

By Josh Smith

Federal cybersecurity officials got a cold reception on Wednesday from House lawmakers on both sides of the aisle who questioned whether White House [cyber proposals](#) could result in abuse and government intrusion. Officials from the Justice, Homeland Security, and Commerce departments who testified before the House Judiciary Subcommittee on Intellectual Property, Competition, and the Internet faced pointed questions about the

[White House Cyberspace Policy Review](#)

unveiled last week. Lawmakers on the panel worried that the administration's plan provides too much government control in cybersecurity issues. The proposal would grant legal immunity to companies who cooperate with federal cyber investigations. That, the subcommittee's ranking member,

Melvin Watt

, D-N.C., said, sounds a lot like the controversial retroactive immunity given to telecom companies that helped in the government's warrantless wiretapping program after the 9/11 terrorist attacks. "These companies could then do something that's unconstitutional just because you say it's not," he said. "People get very uncomfortable with the idea that the government can just call up someone, demand information, and then provide them immunity."

Watt

said that the definition of "critical infrastructure" is too broad and could result in government overreach. He pointed to bipartisan concern over the administration's proposals and said there is much to be done before finalizing any legislation. Rep.

Darrell Issa

, R-Calif., also pressed the witnesses on why the courts wouldn't be more involved in deciding whether to grant immunity to companies. He said the courts are key to keeping the executive branch in check. Although any cooperation with federal officials would be voluntary under the White House proposal, Issa said he is skeptical that such help would be truly free. "You're asking for cooperation with the force of your ability to make life difficult for private companies behind closed doors," Issa told the witnesses. The Homeland Security Department has a history of working well with private companies, said Greg Shaffer, assistant secretary for cybersecurity and communications at DHS. He said the administration is open to working with Congress to develop final legislation. Any cybersecurity legislation should be tailored to prevent overregulation of private industry, said subcommittee Chairman

Bob Goodlatte

, R-Va.. He warned of turning government agencies into "quasi-fiefdoms with absolute authority" over the private sector. "You're asking for a lot of trust from the American people," he said. Beyond legal issues, government involvement in cybersecurity could also hurt economic

innovation, Goodlatte said. “While the government has a crucial role to play, any policy to improve private-sector cybersecurity should not run against or impede our economic prosperity,” he said. “Regulatory mandates are unlikely to [lead to] private-sector cybersecurity improvements and will likely hinder economic growth.” In general, government monitoring of private networks is not included in any of the major cybersecurity bills or in the White House plan, but that risk remains high, said Leslie Harris, president of the Center for Democracy & Technology, who also testified. “Government monitoring of private-to-private communications likely will not occur through the front door,” she said in her opening statement. “Rather, there is a possibility that government monitoring would arise as an indirect result of information-sharing between the private and public sectors, or as an unintended byproduct of programs put in place to monitor communications to or from the government.” Harris said that calling the White House plan another USA PATRIOT Act is an overstatement; but she said she is concerned that the proposal would override decades of privacy laws in the name of information-sharing. Wednesday’s session was the second of at least four congressional hearings on cybersecurity this week. On Monday, members of the [Senate Homeland Security Committee](#) expressed optimism, as well as concerns, about the administration’s cyber plans.