Written by **Brian Koenig** on December 19, 2011

Homeland Security Committee Unveils Cybersecurity Bill

Members of the House Homeland Security Committee unveiled legislation Thursday that would authorize the cybersecurity functions of the Department of Homeland Security (DHS) and establish a quasi-governmental entity to coordinate cybersecurity information-sharing with the private sector. The bill, called the Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act (PrECISE), would station a national clearinghouse for information relating to potential attacks on critical infrastructure, such as electric grid, water facilities, and financial service systems.

"The risk of cyberattack by enemies of the United States is real, is ongoing and is growing," warned Homeland Security Committee Chairman Peter King (R-N.Y., above left). "The PrECISE Act, in line with the framework set forth by the Speaker's Cybersecurity Task Force led by Rep. [Mac] Thornberry [R-Texas], protects our critical infrastructure without a heavy-handed and burdensome regulatory approach that could cost American jobs."

Under Section 226 of the bill, the Secretary of Homeland Security "is authorized to maintain the capability to act as the focal point for cybersecurity through technical expertise and policy development." Further, the Secretary is ordered to "coordinate cybersecurity activities across the Federal Government, designate a lead cybersecurity official within the Department of Homeland Security, publish a cybersecurity strategy and provide appropriate reports to Congress."

In effect, the DHS would identify cybersecurity risks on a sector-by-sector basis and gather existing performance standards to procure the most efficient methods to mitigate identified exposures. The Secretary will review and collect standards and publish cyber-defense information for owners and operators of "covered critical infrastructure," which is defined as the "infrastructure that if destroyed or disabled would result in a significant number of deaths, cause mass evacuations, major disruptions of the economy, or significant disruption to national security."

"Cybersecurity is truly a team sport, and this bill gives DHS needed authorities to play its part in the federal government's cybersecurity mission and enables the private sector to play its part by giving them the information and access to technical support they need to protect critical infrastructure," said Rep. Dan Lungren (R-Calif.), Chairman of the House Cybersecurity Subcommittee.

In addition to Reps. King and Lungren, the bill's original co-sponsors include Rep. Michael McCaul (R-Texas), Rep. Gus Bilirakis (R-Fla.), Rep. Candice Miller (R-Mich.), Rep. Tim Walberg (R-Mich.), Rep. Billy Long (R-Mo.), Rep. Tom Marino (R-Pa.) and Rep. Bob Turner (R-N.Y.) of the Homeland Security Committee, as well as Rep. Steve Stivers (R-Ohio) and Rep. Jim Langevin (D-R.I.).

One key tenet of the legislation is the creation of the National Information Sharing Organization (NISO), a quasi-governmental entity that would be staged as a clearinghouse for exchanging relevant

information regarding cyber threats and vulnerabilities. The organization would be a nonprofit entity consisting of a DHS-appointed board of directors, composed of members from five different federal agencies and 13 members of the private sector.

According to Section 242 of the bill, the NISO would have three primary missions:

> First, facilitating the exchange of cyber threat information, best practices and technical assistance amongst its membership including the Government. Second, it would facilitate the creation of a common operating picture built from information contributed by technically sophisticated members such as the Government, Internet Service Providers, and other members with access to large amounts of network related information. Third, the NISO would act as a catalyst for cooperative research and development of member driven research projects. Additionally, the NISO would incorporate into its membership agreements for the transferability of intellectual property and integrate with the National Cybersecurity and Communications Integration Center at DHS.

All in all, NISO's purpose would be to establish a point of connection between the government and the private sector to pool information about potential cybersecurity threats and to collaborate on methods to prevent such threats from occurring.

While cybersecurity laws have brought a rare agreement between Republicans and Democrats, the two parties have quibbled over certain aspects of the legislation. Generally, House Republicans prefer more limited regulation and discretional incentives to ramp up securities, while Senate Democrats and the White House have suggested more stringent regulations monitored by the DHS.

Many civil liberties groups have expressed concern over cybersecurity legislation such as the PrECISE Act, as these policies could lead to severe privacy rights' violations. Gregory Nojeim, senior counsel at the Center for Democracy & Technology, a public interest organization working to maintain an open and free Internet, believes a completely privately-run organization would be an effective mode to combat cybersecurity threats, but that governmental involvement could lead to unfortunate civil consequences.

For example, under the bill, if a company shares information on a user's Internet activities that it acquired to preclude the user's account from being hacked, the government would have the ability to use that information for its own purposes, including for criminal prosecutions independent of cybersecurity. "This legislation allows for the information to be shared without a court order or other protections," explained Nojeim, referring to a previous version of the PrECISE Act.

Indeed, while NISO would be comprised mostly of private-sector members, companies could have limited authority in the promulgation of rules, and in turn, Nojeim reflected, federal officials could exert considerable influence over NISO's functions.

"Approaches to cybersecurity that would eliminate pseudonymous and anonymous speech online would put privacy at risk, chill free expression and erode the Internet's essential openness," Nojeim asserted in a May 2009 congressional testimony. "As the founders of our country recognized, anonymity and pseudonymity play essential roles in allowing political views to be aired."