

## Energy set to form new group to protect electric grid from cyberattacks

By Jill R. Aitoro 01/05/10

A public-private group the Energy Department is forming to better secure the nation's electric grid from cyberattacks must be given strong regulatory and budgetary authority to drive sweeping changes to computer networks, security specialists said.

In 2009, Congress **said it would give** the department about \$172 million to consider ways to tighten the security of the networks that the energy sector uses to operate the grid once the department formed an independent national organization. Energy has yet to create the group.

Once its launched, the group's goals will be to establish "policies and protocol to ensure the effective deployment of technology and software controls to protect the bulk power electric grid," according to the fiscal 2010 appropriations bill, which President Obama signed into law on Oct. 28, 2009.

Congress required that within 60 days of the enactment of the appropriations law -- which was Dec. 27, 2009 -- Energy Secretary Steven Chu would have to invite qualified individuals from the power and security industries to disseminate best practices in cybersecurity; organize the collection, analysis and dissemination of the vulnerabilities and threats that networks face; and work cooperatively with Energy and other federal agencies that oversee efforts to enhance security of the bulk power electric grid.

Energy plans to conduct a competitive solicitation soon to identify possible participants in the national cybersecurity organization, a spokeswoman said. She could not comment about any steps taken to meet the 60-day deadline set by Congress.

Whether the new organization can successfully protect the grid from attacks will depend on its ability to enforce policies, said Tom Kellermann, vice president of security awareness at Core Security Technologies and former senior data risk management specialist for the treasury security team at the World Bank.

"It is paramount that the department creates this organization with the appropriate authority and resources necessary to both evaluate the risk associated with cyber infiltration of critical energy assets, but also to mitigate the vulnerabilities that are identified," Kellermann said. "There are too many sectors that hide behind plausible deniability" that their network was not the entry point in which a cyberattack successfully infiltrated the grid.

Patricia Hoffman, acting assistant secretary for electricity delivery and energy reliability, **told** the House Energy and Environment Subcommittee in October that "the department recognizes the importance of an independent organization that includes industry in advancing cybersecurity and will make establishing this organization a top priority."

This is not the first organization established to address cybersecurity in the energy sector, noted Gregory Garcia, who served as assistant secretary of cybersecurity and telecommunications at the Homeland Security Department during the Bush administration and now runs his own information security consulting firm, Garcia Strategies. DHS established the Critical Infrastructure Partnership Advisory Council to facilitate coordination among federal, state and local government, and critical infrastructure organizations, for example, and the North American Electric Reliability Corp. is a self-regulatory organization the industry runs that **develops security standards** for individual power plants.

"If the Energy Department would light a fire under [these organizations] to drive the kinds of cyber priorities envisioned in

this legislation and provide funding as appropriate, I think we could move much more quickly with existing resources," he said. "Juggling the steady volley of congressional mandates for new panels, task forces, institutes and councils is an energy-wasting game of whack a mole."