THURSDAY, 3 APRIL 2014 ED Vol 42 • No 64-REV

IHS The Energy Daily

Business and Policy Coverage of the Power, Natural Gas, Oil, Nuclear and Renewable Industries theenergydaily.com

Grid vulnerability leak threatens homeland security cooperation

COMMENTARY

BY PAUL TIAO

Very little has been said about the leak of sensitive details regarding vulnerabilities in our country's electric grid just a few weeks ago. Now, with a bipartisan effort to investigate the leak, I hope it will finally get the attention and action it deserves.

The chair and ranking member of the Senate Energy and Natural Resources Committee, Sens. Mary Landrieu (D-La.) and Lisa Murkowski (R-Alaska), respectively, have called on the Department of Energy's inspector general to investigate the recent leak to the media of details contained in an internal agency memorandum to Jon Wellinghoff, the former chairman of the Federal Energy Regulatory Commission.

The leaked information essentially hands those who would do us harm a roadmap for taking down the grid nationwide. As the current acting chairman of FERC, industry organizations, and now these two senators have pointed out, hostile actors no longer need to develop a strategy for attacking some unknown combination of thousands of transmission substations spread out across the country.

Instead, they now believe that they need only target a handful of key substations in order to take down the entire grid for weeks or even months. The immediate threat is palpable, and the two senators are right to focus the IG's attention on it.

What they are not focusing on, however, is the implications of this leak beyond the immediate threat. In particular, this disclosure undercuts the homeland security partnership that forms the foundation of our nation's safety.

For years, the federal government has been working hard to build a trusting relationship with key critical infrastructure industries that own the energy, water, transportation, and communications facilities that make our country run. The president's recent policy directives underscore this point. Last year's National Infrastructure Protection Plan, presidential policy directive on critical infrastructure security and resilience, and executive order on improving critical infrastructure cybersecurity all emphasized the importance of collaboration, bi-directional information-sharing, joint analysis and coordinated incident response.

In recent years, the FBI, Department of Homeland Security and other agencies have significantly increased the volume and quality of threat information that they share with industry partners. However, persuading companies to share sensitive security information with the government remains a crucial but difficult challenge for government leaders.

Our agency executives push Congress to pass information-sharing laws, exhort potential industry partners to trust them with sensitive industry information, and point to federal laws that protect against the disclosure of sensitive information, but progress towards a true bi-directional flow of sensitive security information has been tough.

Unfortunately, the disclosure of the Wellinghoff memo to the media, in conjunction with February's disclosure of confidential details regarding the 2013 firearms attack on a Pacific Gas & Electric substation in California, has sent a powerful message to industry: The Edward Snowdens of the world may work in any agency, they may be contractors or even current or former government employees, and they may disclose sensitive information about industry security vulnerabilities to the media.

Persuading key industry partners to share information about threats and vulnerabilities just got a lot tougher. The senators' call for an investigation is a step in the right direction. Government must take aggressive action to stop these leaks and protect the workings of those companies that help keep our economy strong and our infrastructure safe. If it does not, we all will surely suffer the consequences.

—Paul Tiao is a partner in the Global Privacy and Cybersecurity Group at Hunton & Williams LLP. He was formerly senior counselor for cybersecurity and technology to FBI Director Robert S. Mueller.