CRS INSIGHT

Vermont Utility Cybersecurity Alarm

January 3, 2017 (IN10631)

|

Related Author

- Richard J. Campbell

|

Richard J. Campbell, Specialist in Energy Policy (rcampbell@crs.loc.gov, 7-7905)

A recent report in the *Washington Post* stated that Russian hackers had penetrated the U.S. electricity grid, after malware said to be associated with a Russian hacking group was found on a Vermont utility company computer. However, a follow-up story in the *Washington Post* quoted U.S. government sources as saying "that the incident is not linked to any Russian government effort to target or hack the utility."

The cybersecurity alarm was raised after a joint report last week by the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) urged electric utilities to search their networks for signs of an infiltration linked to a Russian hacking operation (called the Grizzly Steppe) suspected in the hack of Democratic Party servers. The report listed suspicious Internet addresses, but cautioned that some of the sites might correspond to legitimate activity. The report led an employee at the Burlington Electric Company in Vermont to check his Yahoo email account on his work laptop computer, finding suspicious internet activity. After the utility checked its systems, malware was found on the laptop, but the utility stated that the computer was not connected to the Vermont company's electric grid control system. Federal officials are reported to be still investigating the laptop computer, trying to ascertain how the malware got onto the laptop.

Although the Vermont incident proved not to be as serious a cybersecurity threat as initially reported, there are legitimate concerns with attempts by hackers and others to infiltrate the U.S. electric grid, especially in the wake of the cyberattack on the electric grid in Ukraine in late December 2015. However, most experts believe that the U.S. grid has sufficient redundancies to prevent a major, long-term disruption. The U.S. bulk electric power system is subject to mandatory standards for both cyber and physical security which are enforced by the Federal Energy Regulatory Commission (FERC). Congress gave FERC responsibility for the reliable operations of the grid (including cybersecurity oversight) with the passage of the Energy Policy Act of 2005 (EPACT) (P.L. 109-58).

While there has not been a publicly-reported cybersecurity event or physical attack resulting in a large scale power outage in the United States, the potential for such attacks to cause a wide-scale, long-lasting outage cannot be dismissed. The report from the FBI and DHS was part of a system of regulations, awareness, and best practices intended to detect and remove cybersecurity threats before they can cause damage to systems controlling the U.S. electric grid or other critical infrastructure. It is a specific example of the federal government sharing information about security threats with the appropriate private entities to help ensure the security of privately-owned infrastructure.