Accountability * Integrity * Reliability

Highlights of GAO-12-507T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

February 2012

CYBERSECURITY

Challenges in Securing the Modernized Electricity Grid

Why GAO Did This Study

The electric power industry is increasingly incorporating information technology (IT) systems and networks into its existing infrastructure as part of nationwide efforts—commonly referred to as the "smart grid"—aimed at improving reliability and efficiency and facilitating the use of alternative energy sources such as wind and solar. Smart grid technologies include metering infrastructure ("smart meters") that enable two-way communication between customers and electricity utilities, smart components that provide system operators with detailed data on the conditions of transmission and distribution systems, and advanced methods for controlling equipment. The use of these systems can bring a number of benefits, such as fewer and shorter outages, lower electricity rates, and an improved ability to respond to attacks on the electric grid. However, this increased reliance on IT systems and networks also exposes the grid to cybersecurity vulnerabilities, which can be exploited by attackers. Moreover, for nearly a decade, GAO has identified the protection of systems supporting our nation's critical infrastructure—which include the electric grid—as a governmentwide high-risk area.

GAO is providing a statement describing (1) cyber threats facing cyber-reliant critical infrastructures and (2) key challenges to securing smart grid systems and networks. In preparing this statement, GAO relied on its previously published work in this area.

View GAO-12-507T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or David C. Trimble at (202) 512-3841 or trimbled@gao.gov.

What GAO Found

The threats to systems supporting critical infrastructures are evolving and growing. In a February 2011 testimony, the Director of National Intelligence noted that there had been a dramatic increase in cyber activity targeting U.S. computers and systems in the previous year, including a more than tripling of the volume of malicious software since 2009. Varying types of threats from numerous sources can adversely affect computers, software, networks, organizations, entire industries, and the Internet itself. These include both unintentional and intentional threats, and may come in the form of targeted or untargeted attacks from criminal groups, hackers, disgruntled employees, hostile nations, or terrorists. The interconnectivity between information systems, the Internet, and other infrastructures can amplify the impact of these threats, potentially affecting the operations of critical infrastructures, the security of sensitive information, and the flow of commerce. Moreover, the smart grid's reliance on IT systems and networks exposes the electric grid to potential and known cybersecurity vulnerabilities, which could be exploited by attackers.

As GAO reported in January 2011, securing smart grid systems and networks presented a number of key challenges that required attention by government and industry. These included:

- **A lack of a coordinated approach to monitor industry compliance with voluntary standards.** The Federal Energy Regulatory Commission (FERC) is responsible for regulating aspects of the electric power industry, which includes adopting cybersecurity and other standards it deems necessary to ensure smart grid functionality and interoperability. However, FERC had not, in coordination with other regulators, developed an approach to monitor the extent to which industry will follow the voluntary smart grid standards it adopts. As a result, it would be difficult for FERC and other regulators to know whether a voluntary approach to standards setting is effective.
- **A lack of security features built into smart grid devices.** According to a panel of experts convened by GAO, smart meters had not been designed with a strong security architecture and lacked important security features. Without securely designed systems, utilities would be at risk of attacks occurring undetected.
- **A lack of an effective information-sharing mechanism within the electricity industry.** While the industry has an information-sharing center, it had not fully addressed the need for sharing cybersecurity information in a safe and secure way. Without quality processes for sharing information, utilities may lack information needed to protect their assets against attackers.
- **A lack of metrics for evaluating cybersecurity.** The industry lacked metrics for measuring the effectiveness of cybersecurity controls, making it difficult to measure the extent to which investments in cybersecurity improve the security of smart grid systems. Until such metrics are developed, utilities may not invest in security in a cost-effective manner or be able to make informed decisions about cybersecurity investments.

GAO made several recommendations to FERC aimed at addressing these challenges. The commission agreed with these recommendations and described steps it is taking to implement them.