July 17, 2012

CYBERSECURITY

Challenges in Securing the Electricity Grid

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-926T, a testimony before the Committee on Energy and Natural Resources, U.S. Senate

Why GAO Did This Study

The electric power industry is increasingly incorporating information technology (IT) systems and networks into its existing infrastructure (e.g., electricity networks, including power lines and customer meters). This use of IT can provide many benefits, such as greater efficiency and lower costs to consumers. However, this increased reliance on IT systems and networks also exposes the grid to cybersecurity vulnerabilities, which can be exploited by attackers. Moreover, GAO has identified protecting systems supporting our nation's critical infrastructure (which includes the electricity grid) as a governmentwide high-risk area.

GAO was asked to testify on the status of actions to protect the electricity grid from cyber attacks. Accordingly, this statement discusses (1) cyber threats facing cyber-reliant critical infrastructures, which include the electricity grid, and (2) actions taken and challenges remaining to secure the grid against cyber attacks. In preparing this statement, GAO relied on previously published work in this area and reviewed reports from other federal agencies, media reports, and other publicly available sources.

What GAO Recommends

In a prior report, GAO has made recommendations related to electricity grid modernization efforts, including developing an approach to monitor compliance with voluntary standards. These recommendations have not yet been implemented.

View GAO-12-926T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or David C. Trimble at (202) 512-3841or trimbled@gao.gov.

What GAO Found

The threats to systems supporting critical infrastructures are evolving and growing. In testimony, the Director of National Intelligence noted a dramatic increase in cyber activity targeting U.S. computers and systems, including a more than tripling of the volume of malicious software. 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, 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 electricity grid's reliance on IT systems and networks exposes it to potential and known cybersecurity vulnerabilities, which could be exploited by attackers. The potential impact of such attacks has been illustrated by a number of recently reported incidents and can include fraudulent activities, damage to electricity control systems, power outages, and failures in safety equipment.

To address such concerns, multiple entities have taken steps to help secure the electricity grid, including the North American Electric Reliability Corporation, the National Institute of Standards and Technology (NIST), the Federal Energy Regulatory Commission, and the Departments of Homeland Security and Energy. These include, in particular, establishing mandatory and voluntary cybersecurity standards and guidance for use by entities in the electricity industry. For example, the North American Electric Reliability Corporation and the Federal Energy Regulatory Commission, which have responsibility for regulation and oversight of part of the industry, have developed and approved mandatory cybersecurity standards and additional guidance. In addition, NIST has identified cybersecurity standards that support smart grid interoperability and has issued a cybersecurity guideline. The Departments of Homeland Security and Energy have also played roles in disseminating guidance on security practices and providing other assistance.

As GAO previously reported, there were a number of ongoing challenges to securing electricity systems and networks. These include:

- A lack of a coordinated approach to monitor industry compliance with voluntary standards.
- Aspects of the current regulatory environment made it difficult to ensure the cybersecurity of smart grid systems.
- A focus by utilities on regulatory compliance instead of comprehensive security.
- A lack of security features consistently built into smart grid systems.
- The electricity industry did not have an effective mechanism for sharing information on cybersecurity and other issues.
- The electricity industry did not have metrics for evaluating cybersecurity.