October 21, 2015

CRITICAL INFRASTRUCTURE PROTECTION

Cybersecurity of the Nation's Electricity Grid Requires Continued Attention

GAO Highlights

Highlights of GAO-16-174T, a testimony before the Subcommittees on Energy and Research and Technology, Committee on Science, Space, and Technology, House of Representatives

Why GAO Did This Study

The electric power industry—including transmission and distribution systems—increasingly uses information and communications technology systems to automate actions with the aim of improving the electric grid's reliability and efficiency. However, these "smart grid" technologies may be vulnerable to cyber-based attacks and other threats that could disrupt the nation's electricity infrastructure. Several federal entities have responsibilities for overseeing and helping to secure the electricity grid. Because of the proliferation of cyber threats, since 2003 GAO has designated protecting the systems supporting U.S. critical infrastructure (which includes the electricity grid) as a high-risk area.

GAO was asked to provide a statement on opportunities to improve cybersecurity for the electricity grid. In preparing this statement, GAO relied on previous work on efforts to address cybersecurity of the electric sector.

What GAO Recommends

In its 2011 report, GAO recommended that (1) NIST improve its cybersecurity standards, (2) FERC assess whether challenges identified by GAO should be addressed in ongoing cybersecurity efforts, and (3) FERC coordinate with other regulators to identify strategies for monitoring compliance with voluntary standards. The agencies agreed with the recommendations, but FERC has not taken steps to monitor compliance with voluntary standards.

View GAO-16-174T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

GAO reported in 2011 that several entities—the North American Electric Reliability Corporation (NERC), the National Institute of Standards and Technology (NIST), the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the Department of Energy (DOE)—had taken steps to help secure the electric grid. These included developing cybersecurity standards and other guidance to reduce risks.

While these were important efforts, GAO at that time also identified a number of challenges to securing the electricity grid against cyber threats:

- *Monitoring implementation of cybersecurity standards*: GAO found that FERC had not developed an approach, coordinated with other regulatory entities, to monitor the extent to which the electricity industry was following voluntary smart grid standards, including cybersecurity standards.
- *Clarifying regulatory responsibilities:* The nature of smart grid technology can blur traditional lines between the portions of the grid that are subject to federal or state regulation. In addition, regulators may be challenged in responding quickly to evolving cybersecurity threats.
- *Taking a comprehensive approach to cybersecurity:* Entities in the electricity industry (e.g., utilities) often focused on complying with regulations rather than taking a holistic and effective approach to cybersecurity.
- *Ensuring that smart grid systems have built-in security features:* Smart grid devices (e.g., meters) did not always have key security features such as the ability to record activity on systems or networks, which is important for detecting and analyzing attacks.
- *Effectively sharing cybersecurity information:* The electricity industry did not have a forum for effectively sharing information on cybersecurity vulnerabilities, incidents, threats, and best practices.
- *Establishing cybersecurity metrics:* The electricity industry lacked sufficient metrics for determining the extent to which investments in cybersecurity improved the security of smart grid systems.

Since 2011, additional efforts have been taken to improve cybersecurity in the sector. For example, in 2013, NERC issued updated standards to address these and other cybersecurity challenges. NIST also updated its smart grid cybersecurity standards in 2014. It has also developed a cybersecurity framework for critical infrastructure, and DHS and DOE have efforts under way to promote its adoption. In addition, FERC assessed whether these and other challenges should be addressed in its ongoing cybersecurity efforts. However, FERC did not coordinate with other regulators to identify strategies for monitoring compliance with voluntary cybersecurity standards in the industry, as GAO had recommended. As a result, FERC does not know the extent to which such standards have been adopted or whether they are effective. Given the increasing use of information and communications technology in the electricity subsector and the evolving nature of cyber threats, continued attention can help mitigate the risk these threats pose to the electricity grid.