GAO
Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-117, a report to congressional requesters

January 2011

ELECTRICITY GRID MODERNIZATION

Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed

Why GAO Did This Study

The electric industry is increasingly incorporating information technology (IT) systems into its operations as part of nationwide efforts—commonly referred to as smart grid—to improve reliability and efficiency. There is concern that if these efforts are not implemented securely, the electric grid could become more vulnerable to attacks and loss of services. To address this concern, the Energy Independence and Security Act of 2007 (EISA) provided the National Institute of Standards and Technology (NIST) and Federal Energy Regulatory Commission (FERC) with responsibilities related to coordinating the development and adoption of smart grid guidelines and standards.

GAO was asked to (1) assess the extent to which NIST has developed smart grid cybersecurity guidelines; (2) evaluate FERC's approach for adopting and monitoring smart grid cybersecurity and other standards; and (3) identify challenges associated with smart grid cybersecurity. To do so, GAO analyzed agency documentation, interviewed responsible officials, and hosted an expert panel.

What GAO Recommends

GAO recommends that NIST finalize its plan and schedule for updating its cybersecurity guidelines to incorporate missing elements, and that FERC develop a coordinated approach to monitor voluntary standards and address any gaps in compliance. Both agencies agreed with these recommendations.

View GAO-11-117 or key components.
For more information, contact David A. Powner at (202) 512-9286, pownerd@gao.gov or David C. Trimble at (202) 512-3841, trimbled@gao.gov.

What GAO Found

NIST has developed, and issued in August 2010, a first version of its smart grid cybersecurity guidelines. The agency developed the guidelines—for entities such as electric companies involved in implementing smart grid systems—to provide guidance on how to securely implement such systems. In doing this, NIST largely addressed key cybersecurity elements that it had planned to include in the guidelines, such as an assessment of the cybersecurity risks associated with smart grid systems and the identification of security requirements (i.e., controls) essential to securing such systems. This notwithstanding, NIST did not address an important element essential to securing smart grid systems that it had planned to include—addressing the risk of attacks that use both cyber and physical means. NIST also identified other key elements that surfaced during its development of the guidelines that need to be addressed in future guideline updates. NIST officials said that they intend to update the guidelines to address the missing elements, and have drafted a plan to do so. While a positive step, the plan and schedule are still in draft form. Until the missing elements are addressed, there is an increased risk that smart grid implementations will not be secure as otherwise possible.

In 2010, FERC began a process to consider an initial set of smart grid interoperability and cybersecurity standards for adoption, but has not developed a coordinated approach to monitor the extent to which industry is following these standards. While EISA gives FERC authority to adopt smart grid standards, it does not provide FERC with specific enforcement authority. This means that standards will remain voluntary unless regulators are able to use other authorities—such as the ability to oversee the rates electricity providers charge customers—to enforce them. Additionally, although regulatory fragmentation—the divided regulation over aspects of the industry between federal, state, and local entities—complicates oversight of smart grid interoperability and cybersecurity, FERC has not developed an approach coordinated with other regulators to monitor whether industry is following the voluntary smart grid standards it adopts. FERC officials said they have not yet determined whether or how to do so. Nonetheless, adherence to standards is an important step toward achieving an interoperable and secure electricity system and establishing an approach for coordinating on standards adoption could help address gaps, if they arise.

With respect to challenges to securing smart grid systems, GAO identified the following six key challenges:

• Aspects of the regulatory environment may make it difficult to ensure smart grid systems' cybersecurity.	• Consumers are not adequately informed about the benefits, costs, and risks associated with smart grid systems.
• Utilities are focusing on regulatory compliance instead of comprehensive security.	• There is a lack of security features being built into certain smart grid systems.
• The electric industry does not have an effective mechanism for sharing information on cybersecurity.	• The electricity industry does not have metrics for evaluating cybersecurity.