August 2019

CRITICAL INFRASTRUCTURE PROTECTION

Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid

GAO Highlights

Highlights of GAO-19-332, a report to congressional requesters

Why GAO Did This Study

The nation's electric grid—the commercial electric power generation, transmission, and distribution system comprising power lines and other infrastructure—delivers the electricity that is essential for modern life. As a result, the reliability of the grid—its ability to meet consumers' electricity demand at all times—has been of long-standing national interest.

GAO was asked to review the cybersecurity of the grid. Among other things, this report (1) describes the cybersecurity risks facing the grid, (2) assesses the extent to which DOE has defined a strategy for addressing grid cybersecurity risks, and (3) assesses the extent to which FERC-approved standards address grid cybersecurity risks.

To do so, GAO developed a list of cyber actors that could pose a threat to the grid; identified key vulnerable components and processes that could be exploited; and reviewed studies on the potential impact of cyberattacks on the grid by reviewing prior GAO and industry reports, as well as interviewing representatives from federal and nonfederal entities. GAO also analyzed DOE's approaches to implementing a federal cybersecurity strategy for the energy sector as it relates to the grid and assessed FERC oversight of cybersecurity standards for the grid.

What GAO Recommends

GAO is making three recommendations—one to DOE and two to FERC. (See the next page for information on these recommendations.)

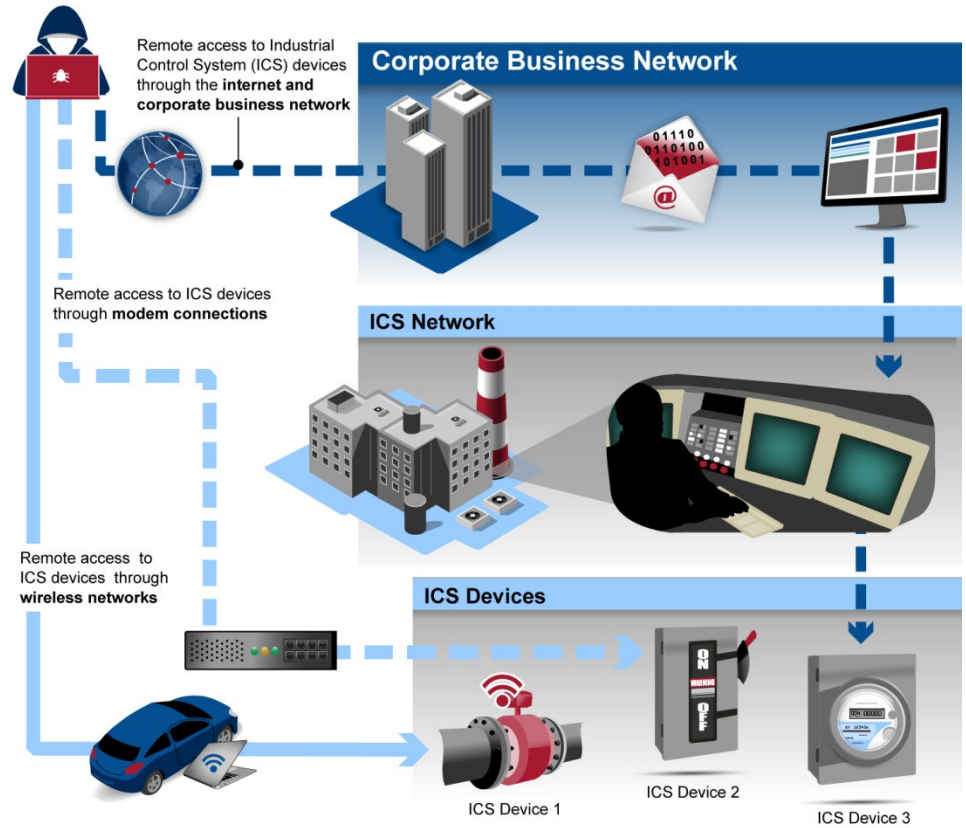
View GAO-19-332. For more information, contact Frank Rusco at (202) 512-3841 or ruscof@gao.gov or Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

The electric grid faces significant cybersecurity risks:

- **Threat actors**. Nations, criminal groups, terrorists, and others are increasingly capable of attacking the grid.
- **Vulnerabilities**. The grid is becoming more vulnerable to cyberattacks—particularly those involving industrial control systems that support grid operations. (The figure below is a high-level depiction of ways in which an attacker could compromise industrial control systems.) The increasing adoption of high-wattage consumer Internet of Things devices—"smart" devices connected to the internet—and the use of the global positioning system to synchronize grid operations are also vulnerabilities.
- **Impacts**. Although cybersecurity incidents reportedly have not resulted in power outages domestically, cyberattacks on industrial control systems have disrupted foreign electric grid operations. In addition, while recent federal assessments indicate that cyberattacks could cause widespread power outages in the United States, the scale of power outages that may result from a cyberattack is uncertain due to limitations in those assessments.

Potential Ways an Attacker Could Compromise Industrial Control System Devices



Source: GAO analysis of Department of Energy and Department of Homeland Security documents. | GAO-19-332

GAO is making a recommendation to DOE to develop a plan aimed at implementing the federal cybersecurity strategy for the grid and ensure that the plan addresses the key characteristics of a national strategy, including a full assessment of cybersecurity risks to the grid.

GAO is also making the following two recommendations to FERC:

1. Consider adopting changes to its approved cybersecurity standards to more fully address the NIST Cybersecurity Framework.

2. Evaluate the potential risk of a coordinated cyberattack on geographically distributed targets and, based on the results of that evaluation, determine if changes are needed in the threshold for mandatory compliance with requirements in the full set of cybersecurity standards.

DOE and FERC agreed with GAO's recommendations.

Although the Department of Energy (DOE) has developed plans and an assessment to implement a federal strategy for addressing grid cybersecurity risks, these documents do not fully address all of the key characteristics needed for a national strategy. For example, while DOE conducted a risk assessment, that assessment had significant methodological limitations and did not fully analyze grid cybersecurity risks. One such key limitation was that the assessment used a model that covered only a portion of the grid and reflected how that portion existed around 1980. Until DOE has a complete grid cybersecurity plan, the guidance the plan provides decision makers in allocating resources to address those risks will likely be limited.

The Federal Energy Regulatory Commission (FERC)—the regulator for the interstate transmission of electricity—has approved mandatory grid cybersecurity standards. However, it has not ensured that those standards fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework. (See table below for an excerpt of GAO's analysis of two of the five framework functions.) Without a full consideration of the framework, there is increased risk that grid entities will not fully implement leading cybersecurity practices.

Extent to Which FERC-Approved Cybersecurity Standards Address the National Institute of Standards and Technology Cybersecurity Framework's Identify and Protect Functions

Function	GAO assessment	Category	GAO assessment
Identify	◑	Asset management	◑
		Business environment	○
		Governance	◑
		Risk assessment	◕
		Risk management strategy	○
		Supply chain risk management	◑
Protect	◕	Identity management, authentication, and access control	●
		Awareness and training	◑
		Data security	◑
		Information protection processes and procedures	◕
		Maintenance	◑
		Protective technology	◑

Legend: ●—Fully address. ◕—Substantially address. ◑—Partially address. ◔—Minimally address. ○—Do not address.

Source: GAO analysis of Federal Energy Regulatory Commission (FERC)-approved cybersecurity standards. | GAO-19-332

In addition, FERC's approved threshold for which entities must comply with the requirements in the full set of grid cybersecurity standards is based on an analysis that did not evaluate the potential risk of a coordinated cyberattack on geographically distributed targets. Such an attack could target, for example, a combination of geographically dispersed systems that each fall below the threshold for complying with the full set of standards. Responding to such an attack could be more difficult than to a localized event since resources may be geographically distributed rather than concentrated in the same area. Without information on the risk of such an attack, FERC does not have assurance that its approved threshold for mandatory compliance adequately responds to that risk.