GAO@100

Highlights

Highlights of GAO-21-81, a report to congressional requesters

March 2021

ELECTRICITY GRID CYBERSECURITY

DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems

Why GAO Did This Study

Protecting the reliability of the U.S. electricity grid, which delivers electricity essential for modern life, is a long-standing national interest. The grid comprises three functions: generation, transmission, and distribution. In August 2019, GAO reported that the generation and transmission systems—which are federally regulated for reliability—are increasingly vulnerable to cyberattacks.

GAO was asked to review grid distribution systems' cybersecurity. This report (1) describes the extent to which grid distribution systems are at risk from cyberattacks and the scale of potential impacts from such attacks, (2) describes selected state and industry actions to improve distribution systems' cybersecurity and federal efforts to support those actions, and (3) examines the extent to which DOE has addressed risks to distribution systems in its plans for implementing the national cybersecurity strategy. To do so, GAO reviewed relevant federal and industry reports on grid cybersecurity risks and analyzed relevant DOE documents. GAO also interviewed a nongeneralizable sample of federal, state, and industry officials with a role in grid distribution systems' cybersecurity.

What GAO Recommends

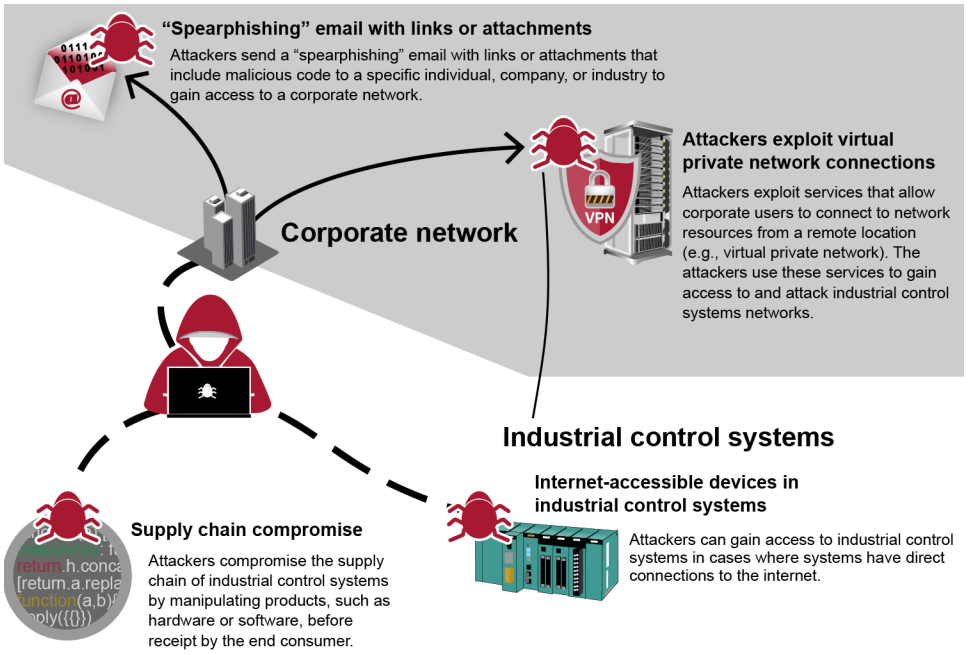
GAO recommends that DOE more fully address risks to the grid's distribution systems from cyberattacks—including their potential impact—in its plans to implement the national cybersecurity strategy. DOE agreed with GAO's recommendation.

View GAO-21-81. For more information, contact Frank Rusco at (202) 512-3841or ruscof@gao.gov or Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

The U.S. grid's distribution systems—which carry electricity from transmission systems to consumers and are regulated primarily by states—are increasingly at risk from cyberattacks. Distribution systems are growing more vulnerable, in part because their industrial control systems increasingly allow remote access and connect to business networks. As a result, threat actors can use multiple techniques to access those systems and potentially disrupt operations. (See fig.) However, the scale of potential impacts from such attacks is not well understood.

Examples of Techniques for Gaining Initial Access to Industrial Control Systems



Source: GAO analysis of industry and federal documents. | GAO-21-81

Distribution utilities included in GAO's review are generally not subject to mandatory federal cybersecurity standards, but they, and selected states, had taken actions intended to improve distribution systems' cybersecurity. These actions included incorporating cybersecurity into routine oversight processes and hiring dedicated cybersecurity personnel. Federal agencies have supported these actions by, for example, providing cybersecurity training and guidance.

As the lead federal agency for the energy sector, the Department of Energy (DOE) has developed plans to implement the national cybersecurity strategy for the grid, but these plans do not fully address risks to the grid's distribution systems. For example, DOE's plans do not address distribution systems' vulnerabilities related to supply chains. According to officials, DOE has not fully addressed such risks in its plans because it has prioritized addressing risks to the grid's generation and transmission systems. Without doing so, however, DOE's plans will likely be of limited use in prioritizing federal support to states and industry to improve grid distribution systems' cybersecurity.