United States Government Accountability Office

Report to Congressional Requesters

March 2021

ELECTRICITY GRID CYBERSECURITY

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

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-81

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

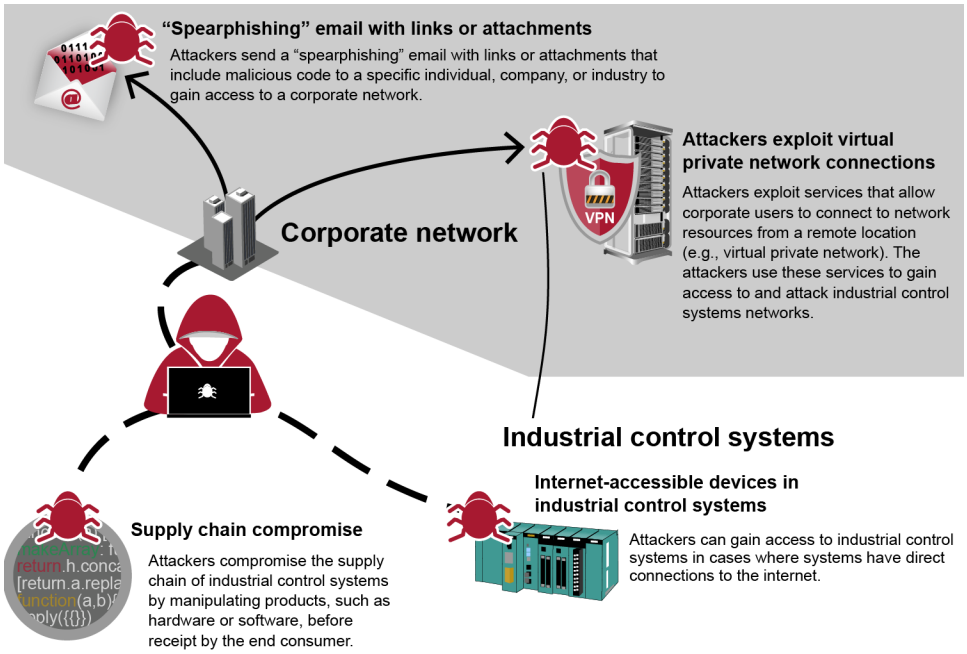
GAO recommends that DOE more fully address risks to the grid's distribution systems from cyberattacks—including their potential impact—in its plans to implement the national cybersecurity strategy. DOE agreed with GAO's recommendation.

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.

Contents

Tables

Figures

Abbreviations

DOE	Department of Energy
DHS	Department of Homeland Security
FERC	Federal Energy Regulatory Commission
GPS	global positioning system
IT	information technology
NIST	National Institute of Standards and Technology
NERC	North American Electric Reliability Corporation

441 G St. N.W.
Washington, DC 20548

March 18, 2021

The Honorable Eddie Bernice Johnson
Chairwoman
Committee on Science, Space, and Technology
House of Representatives

The Honorable Donald S. Beyer, Jr.
House of Representatives

The Honorable Marc A. Veasey
House of Representatives

The nation's electricity grid delivers the electricity that is essential for modern life. Consequently, the reliability of the grid—its ability to meet consumers' electricity demand at all times—has been of long-standing national interest. A recently discovered and ongoing significant cyber incident, likely of Russian origin according to the U.S. Intelligence Community, highlights the importance of securing U.S. critical infrastructure, including the grid.[1]

The U.S. electricity grid comprises three distinct functions: generation, transmission, and distribution. The generation and transmission systems, which together make up the bulk power system,[2] are federally regulated for reliability. In August 2019, we reported that the bulk power system is becoming more vulnerable to cyberattacks and that additional federal actions are needed to address cybersecurity risks facing the grid.[3]

The reliability of the grid's distribution systems—which carry electricity between the transmission system and industrial, commercial, or

[1]The extensive incident was discovered in December 2020 and compromised the networks of several federal agencies, critical infrastructure entities, and private sector organizations.

[2]"Bulk power system" refers to (1) facilities and control systems necessary for operating the electric transmission network and (2) the output from certain generation facilities needed for reliability.

[3]GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019).

residential consumers—is generally regulated by the states.[4] Nevertheless, the federal government is responsible for outlining a national strategy for critical infrastructure cybersecurity that includes the grid's distribution systems. Further, federal agencies, including the Department of Energy (DOE) and the Department of Homeland Security (DHS), have roles in helping to secure those systems. For example, in 2013, the President directed federal agencies to work with owners and operators of critical infrastructure and with state, local, tribal, and territorial governments to take proactive steps to manage risk and strengthen the security of critical infrastructure from all hazards, including cyberattacks.[5] DOE was designated as the lead agency for the energy sector. DHS was given responsibility to coordinate the federal effort to promote the security and resilience of the nation's critical infrastructure, including the grid.

Ensuring the cybersecurity of the nation has been on our High-Risk List since 1997, and we expanded this area to include the protection of critical cyber infrastructure, including the grid, in 2003.[6] In September 2018, we issued an update that identified actions needed to address cybersecurity challenges facing the nation, including development of a more comprehensive national strategy and better oversight of national cybersecurity.[7] We later identified ensuring national cybersecurity as one of nine high-risk areas that need especially focused executive and congressional attention.[8]

You asked us to evaluate the cybersecurity risks to the grid's distribution systems and their connection to the broader electricity grid as well as the actions federal, state, and other entities have taken to address these risks. This report (1) describes the extent to which the grid's distribution systems are at risk from cyberattacks and the scale of potential impacts from such attacks, (2) describes selected state and industry actions to

[4]The U.S. electricity grid, including its distribution systems, extends into parts of Canada and Mexico, which may have different governance structures.

[5]White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

[6]GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 16, 2017).

[7]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation,* GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[8]GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas,* GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

improve distribution systems' cybersecurity and federal efforts to support those actions, and (3) examines the extent to which DOE has addressed risks to grid distribution systems from cyberattacks in its plans for implementing the national cybersecurity strategy for the energy sector.

To address the first two objectives, we conducted semistructured interviews with 38 key federal and nonfederal entities that play a role in grid distribution systems' cybersecurity:

- **Federal entities**
  - Officials from four federal agencies with responsibilities related to distribution systems' cybersecurity (e.g., DOE, DHS) that we identified from previous GAO reports; and
  - Officials from nine national laboratories that we selected based on previous or ongoing research and development projects related to grid distribution systems (e.g., Argonne, Brookhaven, Idaho) and identified from previous GAO reports and recommendations from federal officials.
- **Nonfederal entities**
  - State officials from six public utility commissions (henceforth referred to as "states" or "commissions") that we selected based on multiple criteria, including operating in states that contain all distribution utility ownership types;[9] and
  - Industry representatives from six distribution utilities (henceforth referred to as "utilities") that we selected based on multiple criteria, including being located in one of the states of the six selected public utility commissions and designation as critical infrastructure by DHS; as well as seven electric industry associations, two cybersecurity firms; three grid equipment manufacturers; and one researcher, all of whom we identified from previous GAO reports and recommendations from entities we interviewed and selected because of their relevant knowledge of grid distribution systems' cybersecurity.

The views of the officials and representatives we interviewed cannot be generalized to those we did not speak with as part of our review, but they provide valuable insight into the extent to which the grid's distribution systems are at risk from cyberattacks and actions intended to improve

[9]Distribution utilities are distinguished by three primary ownership types—investor owned, publicly owned (e.g., municipal utilities), and cooperatives.

distribution systems' cybersecurity. We conducted a content analysis of these entities' interview responses to identify any themes related to managing grid distribution systems' cybersecurity risks.

To describe the extent to which the grid's distribution systems are at risk from cyberattacks and the scale of potential impacts from such attacks, we reviewed threat assessments from relevant federal agencies.[10] We also reviewed our prior reports on grid cybersecurity and relevant reports from DOE and DHS.[11]

To describe selected state and utility actions to improve distribution systems' cybersecurity and federal efforts to support those actions, we reviewed relevant documentation from these entities, such as emergency management plans, research project descriptions, and state cybersecurity legislation.

To examine the extent to which DOE has addressed risks to grid distribution systems from cyberattacks in its plans for implementing the national cybersecurity strategy for the energy sector, we reviewed and analyzed relevant DOE plans and assessments.[12] We also incorporated findings from our prior work that compared those plans and assessments with leading practices GAO identified on key characteristics for a national

[10]For example, Daniel R. Coats, Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, testimony before the Senate Select Committee on Intelligence, 116th Cong., 1st sess., January 29, 2019; Department of Energy, Office of Electricity Delivery and Energy Reliability, *Electric Subsector Risk Characterization Study* (Washington, D.C.: June 2017); and Department of Homeland Security*, 2020 Homeland Threat Assessment* (Washington, D.C.: October 2020).

[11]For example, GAO*, Cybersecurity: Challenges in Securing the Electric Grid,* GAO-12-926T (Washington, D.C.: July 17, 2012); Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Securing Industrial Control Systems: A Unified Initiative FY2019 – 2023* (Washington, D.C.: July 2020); and Department of Energy, Office of Inspector General, *Audit Report: Federal Energy Regulatory Commission's Monitoring of Power Grid Cyber Security,* DOE/IG-0846 (Washington, D.C.: January 2011).

[12]Department of Energy, *EERE* [Energy Efficiency and Renewable Energy] *Cybersecurity Multiyear Program Plan* (Washington, D.C.: October 2020); *Multiyear Plan for Energy Sector Cybersecurity* (Washington, D.C.: May 2018); Department of Energy and Department of Homeland Security, *Assessment of Electricity Disruption Incident Response Capabilities* (Washington, D.C.: August 2017); and Department of Energy and Department of Homeland Security, *Energy Sector-Specific Plan, 2015* (Washington, D.C.: 2015).

strategy.[13] Appendix I provides further information about the scope of our review and the methods we used.

We conducted this performance audit from September 2019 to March 2021, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

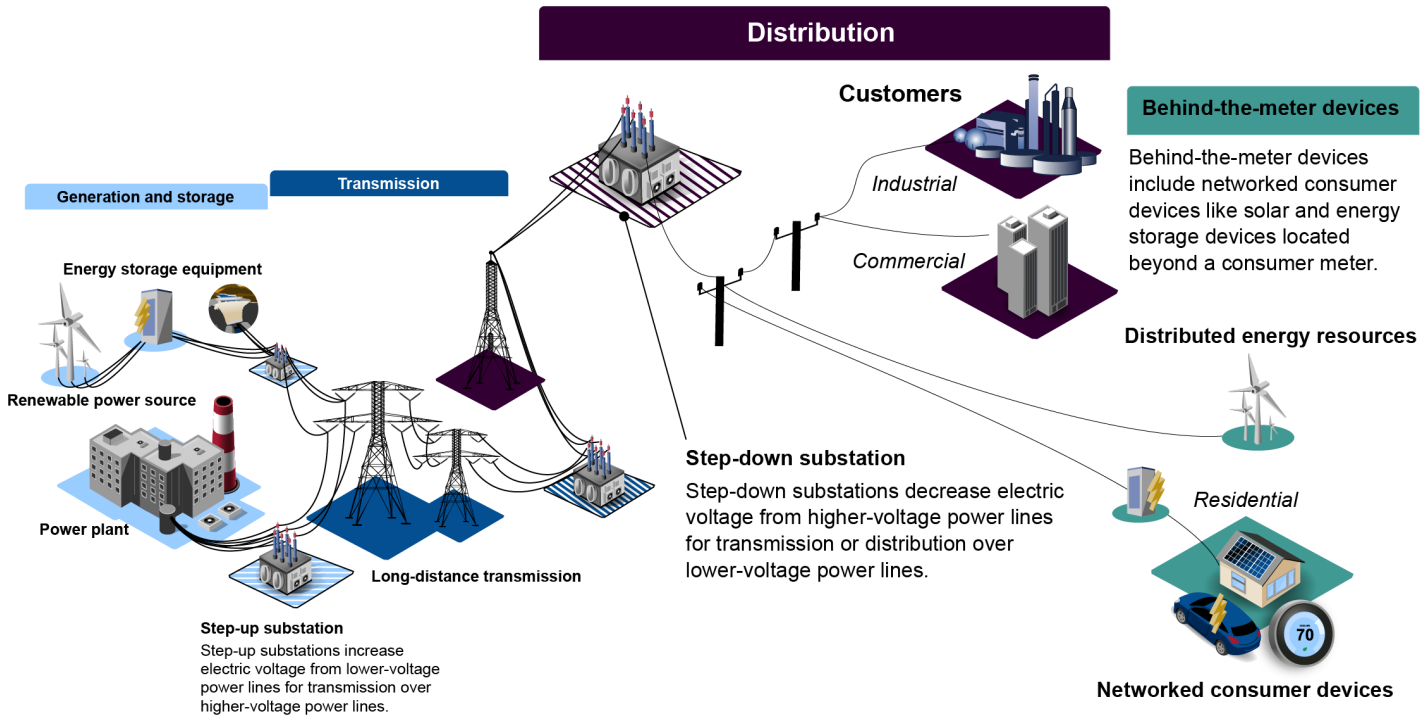
Grid Components and Functions

As shown in figure 1, the U.S. electricity grid comprises three distinct functions:

- **Generation and storage:** Power plants generate electric power by converting energy from other forms—chemical, mechanical (hydroelectric or wind), thermal, radiant energy (solar), or nuclear—into electric power. Energy storage, such as batteries or pumped hydroelectric, can improve the operating capabilities of the grid while also regulating the quality and reliability of power.
- **Transmission:** The grid's transmission system connects geographically distant power plants with areas where electric power is consumed. Substations are used to transmit electricity at varied voltages. These substations generally contain a variety of equipment and system operations instruments to control the flow of electric power.
- **Distribution:** The grid's distribution systems carry electric power out of the transmission system to industrial, commercial, residential, and other consumers. Distribution systems may have distributed energy resources (e.g., solar panel installations on homes and businesses), smart meters, and networked consumer devices (e.g., smart thermostats and electric vehicle chargers) connected to them.

[13]GAO-19-332.

Figure 1: Functions of the U.S. Electricity Grid



Sources: GAO; Art Explosion (images). | GAO-21-81

Distribution Systems' Cybersecurity Regulation

Distribution utilities are generally not subject to the mandatory federal cybersecurity standards that apply to the bulk power system.[14] Instead, state and local entities typically oversee the reliability of the grid's distribution systems, and distribution utilities may apply national cybersecurity guidance and standards voluntarily.[15] Distribution utilities are distinguished by three primary ownership types:

[14]The Federal Energy Regulatory Commission (FERC)—the federal regulator for the interstate transmission of electricity—has approved mandatory cybersecurity standards for the bulk power system. FERC's regulatory authority and responsibility specifically excludes facilities used in the local distribution of electricity.

[15]In addition, state public utility commissions may adopt Institute of Electrical and Electronics Engineers standards on a voluntary or mandatory basis, and distribution utilities may voluntarily implement the standards, according to FERC officials.

- **Investor-owned** distribution utilities are privately owned. They are overseen by state public utility commissions.
- **Publicly owned** (e.g., municipal) distribution utilities are divisions of local government. They are overseen by local city councils or by elected or appointed boards.
- **Cooperatives** are private, member-owned utilities legally established to be owned by and operated for the benefit of those using its service. Cooperatives tend to serve rural populations and are overseen by their members.

Industrial Control Systems

Industrial control systems play a significant role in supporting the control of electric power generation, transmission, and—increasingly—distribution. These vital systems monitor and control sensitive processes and physical functions, such as the opening and closing of circuit breakers on the grid. Early industrial control systems were not designed with cybersecurity protections in mind because they operated in isolation and were not connected to information technology (IT) systems or the internet. Technological advances in these systems have offered advantages to system operators but have also increased the vulnerability of the systems. For example, increased access to industrial control systems, particularly through remote means and IT networking protocols, offers benefits to system operators such as easier maintenance and more detailed systems data, but they also make these systems more vulnerable to cyberattacks. Such cyberattacks may require an unusual degree of sophistication and knowledge, in part because industrial control systems often use operating systems and applications that may be unfamiliar to typical IT personnel.

Critical Infrastructure Protection Roles and Responsibilities

Federal policy and public-private plans establish roles and responsibilities for the protection of critical infrastructure, including the electricity grid. For example:

- **Presidential Policy Directive 21** made DOE responsible for collaborating with critical infrastructure owners and operators in the energy sector, identifying vulnerabilities, and helping to mitigate

incidents.[16] The directive also called for DHS to coordinate the overall federal effort to promote the security and resilience of the nation's critical infrastructure. The directive emphasized that critical infrastructure owners and operators (e.g., distribution utilities) are uniquely positioned to manage risks to their individual operations and assets and to determine effective strategies to make them more secure and resilient.

- **The National Infrastructure Protection Plan** further integrates critical infrastructure protection efforts between government and private sectors by describing a voluntary public-private partnership. Under this partnership, designated agencies serve as the lead coordinators for the security programs of their respective sectors.[17] This plan made designated agencies responsible for the development and updating of a critical infrastructure plan to support the National Infrastructure Protection Plan.
- **The National Defense Authorization Act for Fiscal Year 2021** establishes additional roles and responsibilities for designated agencies in securing critical infrastructure.[18] For example, the act requires designated agencies to provide specialized expertise, assess risks, and support risk management of their respective critical infrastructure sectors.

[16]White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013). DOE has this role through its designation as the sector-specific agency for the energy sector. The Fixing America's Surface Transportation Act (FAST Act) codified DOE's role and gave it the authority to order emergency measures, following a presidential declaration of a grid security emergency, to protect or restore the reliability of critical electric infrastructure. Pub. L. No. 114-94, Div. F, § 61003, 129 Stat. 1312, 1778 (2015).The FAST Act contains provisions designed to protect and enhance the nation's electric power delivery infrastructure.

[17]Department of Homeland Security*, NIPP* [National Infrastructure Protection Plan] *2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).The plan also called for each sector to have a government coordinating council, consisting of representatives from various levels of government, and many sectors have a coordinating council consisting of owner-operators of these critical assets or representatives of their respective trade associations. For example, the Energy Sector Government Coordinating Council has been established (comprising the electricity subsector, as well as the oil and natural gas subsectors), and an Electricity Subsector Coordinating Council has been established to represent electricity asset owners and operators.

[18]The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 9002(c)(1), 134 Stat. 3388, 4770–72.

National Cybersecurity Strategy

The executive branch has taken steps toward outlining a national strategy for confronting cyber threats to critical infrastructure—including the grid's distribution systems. For example, in 2017, the White House issued Executive Order 13800, which required DOE and DHS to assess the potential impacts of a significant cyber incident.[19] Additionally, in 2018, the National Security Council issued the *National Cyber Strategy*, which describes actions that federal agencies and the administration are to take, such as prioritizing risk-reduction across seven key areas, including energy and power, to protect critical infrastructure.[20]

DOE has led the development of three plans and an assessment that, collectively, represent the department's efforts to implement the national cybersecurity strategy specifically for the energy sector, including the grid:

- **The Energy Sector Specific Plan** was developed in 2015 in response to Presidential Policy Directive 21. The plan guides efforts to improve the security and resilience of the energy sector—including the electricity grid—and discusses the various cyber and physical risks and threats facing the sector.[21]
- **Assessment of Electricity Disruption Incident Response Capabilities**, developed in 2017 in response to Executive Order 13800, examines the potential scope and duration of a cyberattack on the electricity grid.[22] It also evaluates the nation's readiness to manage the impacts of a cyber incident and assesses capability gaps in responding to an incident.

[19]Executive Order No. 13800, 82 Fed. Reg. 22,391 (May 16, 2017). The executive order also required DOE and DHS to assess the readiness of the United States to manage the consequences of such an incident and any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident.

[20]White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: September 2018). In 2019, the National Security Council developed an Implementation Plan that details activities that federal entities are to undertake to execute the priority actions outlined in the National Cyber Strategy. However, we reported in September 2020 that the Implementation Plan and National Cyber Strategy, when combined, are missing key elements for addressing some characteristics of a national strategy. GAO, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GAO-20-629 (Washington, D.C.: Sept. 22, 2020).

[21]Department of Energy and Department of Homeland Security, *Energy Sector-Specific Plan, 2015.*

[22]Department of Energy and Department of Homeland Security, *Assessment of Electricity Disruption Incident Response Capabilities.*

- **The Multiyear Plan for Energy Sector Cybersecurity** that DOE developed in 2018 lays out an integrated strategy to reduce cyber risks in the U.S. energy sector through high-priority activities that are to be coordinated within DOE and with the strategies, plans, and activities of other federal agencies and the energy sector.[23] It also describes how DOE will carry out its mandated cybersecurity responsibilities and address the evolving security needs of energy owners and operators.[24]
- **The 2020 Cybersecurity Multiyear Program Plan** supplements the 2018 multiyear program plan and describes DOE's strategy and activities for energy delivery systems within its purview.[25] The plan includes milestones and time lines for the completion of these activities.

In August 2019, we reported that these first two DOE plans and assessment to implement the national cybersecurity strategy for the grid did not fully address all of the key characteristics needed to implement a national strategy.[26] For example, none of those documents fully analyzed the cybersecurity risks and challenges to the grid. In response, we recommended that DOE develop a plan that addresses the key characteristics of a national strategy, including a full assessment of cybersecurity risks to the grid. DOE agreed with our recommendation and, according to DOE officials, the department is updating its plans and assessment.

[23]Department of Energy, *Multiyear Plan for Energy Sector Cybersecurity.*

[24]DOE established the Office of Cybersecurity, Energy Security, and Emergency Response in 2018 with the goal of providing greater visibility, accountability, and flexibility in securing U.S. energy infrastructure.

[25]Department of Energy, *EERE Cybersecurity Multiyear Program Plan.*

[26]GAO-19-332.

The Grid's Distribution Systems Are Increasingly at Risk from Cyberattacks, but the Scale of Potential Impacts Is Unclear

The grid's distribution systems face significant cybersecurity risks—that is, threats, vulnerabilities, and impacts—and are increasingly vulnerable to cyberattacks. Threat actors are growing more adept at exploiting these vulnerabilities to execute cyberattacks.[27] However, the scale of the potential impacts of such cyberattacks on the grid's distribution systems is unclear.

Grid Distribution Systems Are Increasingly Vulnerable to Cyberattacks

Like the rest of the grid, distribution systems are becoming more vulnerable to cyberattacks, in part due to the introduction of and reliance on monitoring and control technologies. For example,

- industrial control systems increasingly include remote access capabilities to monitor and control operations and connect to corporate business networks;
- grid operations increasingly rely on global positioning systems (GPS) for critical position, navigation, and timing information; and
- more networked consumer devices and distributed energy resources, which provide increased monitoring and control capabilities for consumers and utilities, are being connected to distribution systems networks.[28]

Increasing grid vulnerabilities related to these technological advances, discussed in further detail below, are compounded for distribution systems because the sheer size and dispersed nature of the systems present a large attack surface.

Industrial Control Systems

According to officials and representatives of selected federal and nonfederal entities we interviewed, industrial control systems in grid distribution systems are becoming increasingly vulnerable to cyberattacks. For example, officials from two selected national laboratories and a cybersecurity firm stated that the addition of remote access capabilities and connections to business IT networks could make

[27]A threat actor is a person or group that takes malicious action—including a cyberattack—on computers, systems, or networks.

[28]GAO-19-332.

industrial control systems more vulnerable and increase the attack surface of distribution systems.

According to MITRE's widely accepted framework for classifying cyberattacks on industrial control systems, threat actors can use multiple techniques to gain initial access to industrial control systems.[29] Table 1 describes publicly reported examples of such techniques, and figure 2 illustrates these techniques.[30]

[29]MITRE Corporation, Main Page, "ATT&CK® for Industrial Control Systems," last modified on June 3, 2020, https://collaborate.mitre.org/attackics/index.php/Main_Page. The MITRE ATC&CK® Framework for Industrial Control Systems is an overview of the tactics and techniques, including corresponding examples, that could be used to attack industrial control systems. It defines a technique as the way in which a threat actor achieves their goal by performing an action.

[30]Some of the examples included in table 1 do not directly relate to the grid's distribution systems, but they reflect examples of attacks on industrial control systems generally that may be relevant to industrial control systems used in the grid's distribution systems.

Table 1: Examples of Techniques for Gaining Initial Access to Industrial Control Systems

Description	Examples
Attackers exploit internet-accessible devices in industrial control systems.	In 2012, attackers used automated tools to discover General Electric industrial control systems devices connected to the internet.[a] The attackers then exploited this connection to infect the devices with malware.[b]
Attackers compromise the supply chain[c] of industrial control systems by manipulating products (such as hardware or software) or delivery mechanisms before receipt by the end consumer.	In 2018, Schneider Electric issued an alert regarding certain solar system monitoring devices that were packaged with universal serial bus removable media that one of its suppliers contaminated with malware during manufacturing.[d] According to a Finnish cybersecurity company, in 2014, a group of attackers used malware to compromise the software installers for industrial control systems devices available on the websites of three vendors based in Europe. According to the cybersecurity company's research, this malware infected multiple organizations in Europe and at least one company in California. The malware reportedly gathered information about other industrial control systems devices connected to the infected devices and sent this information to servers that the malicious actors controlled.
Attackers send a "spearphishing" email with links or attachments that include malicious code to a specific individual, company, or industry to gain access to a corporate network.	According to a report from the Electricity Information Sharing and Analysis Center and the SANS Institute, in 2015, malicious actors sent spearphishing emails with malware embedded in Microsoft Word attachments to users on three Ukrainian electricity utilities' business information technology (IT) networks.[e] When users opened the Microsoft Word attachments, the malware was installed on the users' systems.
Attackers exploit services that allow users to connect to network resources from a remote location (e.g., virtual private network[f]). The attackers use these services to gain access to and attack industrial control systems networks.	After gaining initial access to the business IT networks of the three regional Ukrainian electricity distribution utilities in 2015, attackers compromised the virtual private networks that the utilities used to connect the business IT networks to the industrial control systems networks.[g] This compromise was enabled by the attacker's harvesting of legitimate credentials from the business IT network and using the credentials to access the virtual private network, which likely did not require multifactor authentication.[h]

Source: GAO analysis and summary of relevant documents. | GAO-21-81

[a]National Institute of Standards and Technology (NIST) guidance on industrial control systems security strongly encourages organizations not to directly expose industrial control systems devices to the internet. National Institute of Standards and Technology, Guide to Industrial Control Systems (ICS) Security, NIST 800-82 Rev. 2 (Gaithersburg, MD: May 2015). Yet search engines that catalog industrial control systems (e.g., Shodan) suggest that industrial control systems remain directly exposed to the internet.

[b]Cybersecurity and Infrastructure Security Agency, ICS Alert: Ongoing Sophisticated Malware Campaign Compromising ICS (ICS-ALERT-14-281-01E), accessed September 25, 2020, https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-14-281-01B

[c]The supply chain is a linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of products and services and extends through development, sourcing, manufacturing, handling, and delivery of products and services to the acquirer.

[d]Schneider Electric, Security Notification – USB Removable Media Provided with Conext Combox and Conext Battery Monitor (Andover, MA.: Aug, 24, 2018).

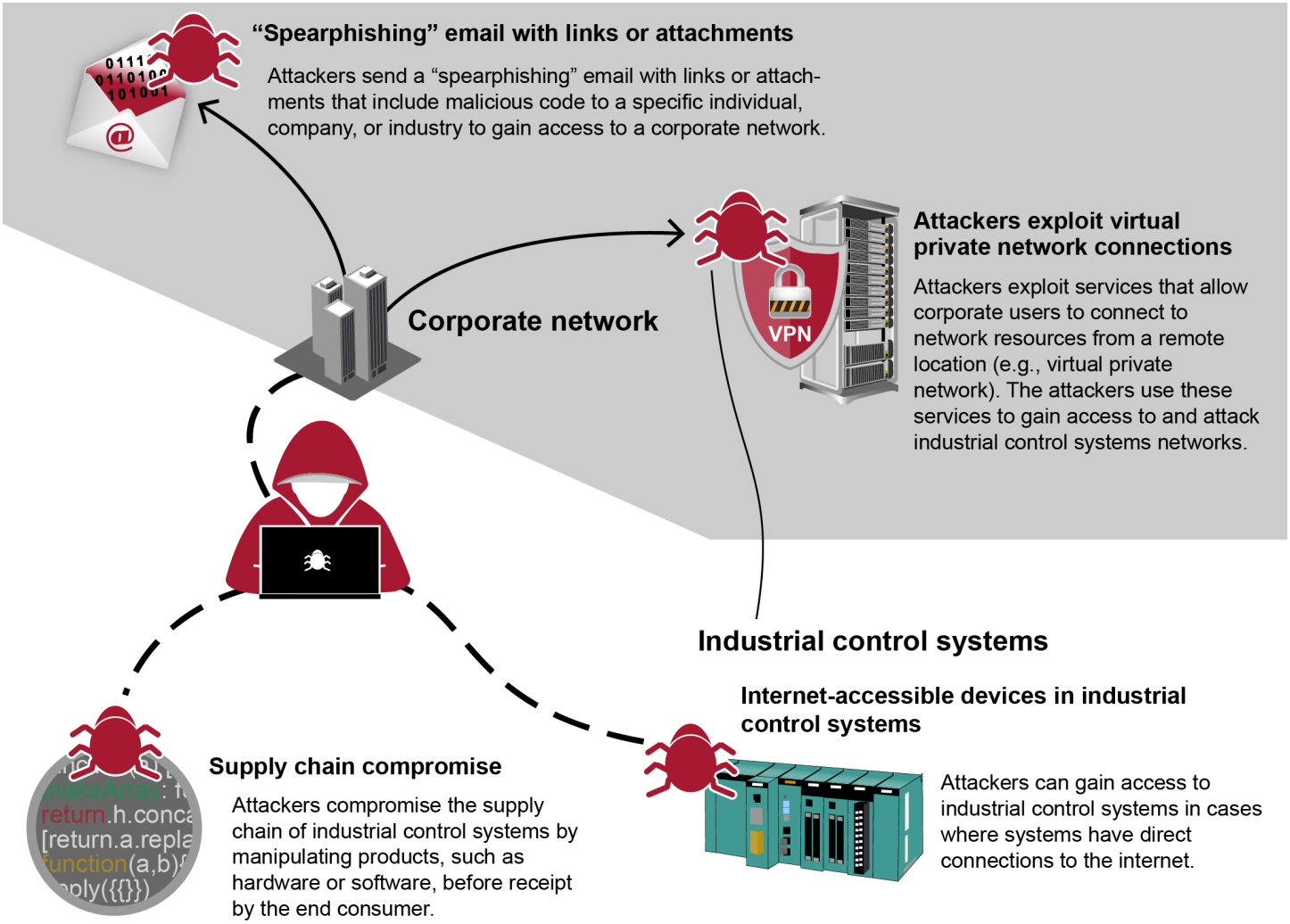
[e]SANS Industrial Control Systems, Analysis of the Cyber Attack on the Ukrainian Power Grid (North Bethesda, MD.: Mar, 18, 2016).

[f]A virtual private network is a logical network connection that overlays existing physical networks to provide secure transmission of data.

[g]SANS Industrial Control Systems, Analysis of the Cyber Attack on the Ukrainian Power Grid.

[h]Multifactor authentication uses two or more different factors to achieve authentication. Factors may include (i) something the user knows (e.g., password/PIN); (ii) something the user has (e.g., cryptographic identification device, token); or (iii) something the user is (e.g., biometric factor).

Figure 2: Examples of Techniques for Gaining Initial Access to Industrial Control Systems



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

According to the MITRE cyberattack framework, after gaining initial access to industrial control systems, attackers may use other tactics—such as execution (i.e., running malicious code), evasion (i.e., avoiding detection), and lateral movement (i.e., moving through the industrial control systems environment)—to position themselves to achieve their ultimate goals of manipulation or interruption of industrial control systems. Federal and nonfederal entities we interviewed noted that the grid's distribution systems—including industrial control systems—may be

vulnerable to these tactics as part of cyberattacks because of poor cybersecurity practices at utilities related to encryption,[31] authentication,[32] patch management,[33] and configuration management.[34]

As we have previously reported,[35] these and other vulnerabilities in grid industrial control systems may also stem from factors such as the following:

- Older legacy systems were not designed with cybersecurity protections because they were not intended to connect to networks such as the internet. For example, many legacy devices are not able to authenticate commands to ensure that they have been sent from a valid user and may not be capable of running modern encryption protocols. In addition, some legacy devices do not have the capability to log commands sent to the devices, making it more difficult to detect malicious activity. Further, older legacy systems often rely on unsupported operating systems that no longer receive modern software security patches to address vulnerabilities, according to DHS officials. The officials noted, for example, that Microsoft stopped supporting Windows XP with security patches in 2014, but many industrial control systems still used the unsupported operating system at that time.

[31]NIST defines encryption as the translation of data into a form that is unintelligible without a deciphering mechanism. National Institute of Standards and Technology, *Security Guide for Interconnecting Information Technology Systems*, NIST SP 800-47 (Gaithersburg, MD.: August 2002).

[32]NIST defines authentication as the verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Rev. 5 (Gaithersburg, MD.: January 2015).

[33]NIST defines patch management as the systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, NIST SP 800-137 (Gaithersburg, MD.: September 2011).

[34]NIST defines configuration management as a collection of activities focused on establishing and maintaining the integrity of industrial control systems, through control of processes for initializing, changing, and monitoring the configurations of those products. National Institute of Standards and Technology, *Security and Privacy Controls.*

[35]GAO-19-332.

- Safety and efficiency goals of the grid conflict with the goal of security in the design and operation of the systems. For example, vulnerability scanning is often used in IT systems to validate proper system configuration and to identify any vulnerabilities that may be present. However, grid operators often do not use conventional IT vulnerability scanning because of perceptions that it can impact the availability of energy delivery systems,[36] and testing may not always detect vulnerabilities present in industrial control systems.
- Systems components often have to be taken offline so that owners and operators can apply security patches to address known cybersecurity vulnerabilities. However, this may not happen in a timely manner because the devices must remain highly available to support the reliable operation of the grid.

Because of the previously mentioned vulnerabilities, it may be possible for attackers to manipulate, interrupt, or disrupt distribution utilities' physical control processes or industrial control systems to cause disruptions, according to MITRE's framework for classifying cyberattacks on industrial control systems. Table 2 below describes four publicly reported examples of impacts from cyberattacks on industrial control systems, including cyberattacks on grid distribution systems.[37]

[36]According to DHS officials, this is a common misconception based on an outdated 2005 national laboratory report. The officials added that a more recent national laboratory report found that vulnerability scanning is not likely to have a detrimental effect on the safety and resilience of energy delivery systems. Lawrence Livermore National Laboratory, *Safe Active Scanning for Energy Delivery Systems: Final Report*, LLNL-TR-740556 (Livermore, CA: Sept. 30, 2017).

[37]Some of the examples included in table 2 do not directly relate to grid distribution systems but reflect examples of cyberattacks on industrial control systems generally that may be relevant to industrial control systems used in the grid's distribution systems.

Table 2: Potential Impacts of Cyberattacks on Industrial Control Systems

Impact	Description[a]	Example
Performance of unauthorized actions by systems devices	Command messages are used in industrial control systems networks to give direct instructions to devices. Attackers may send unauthorized command messages to instruct industrial control systems devices to perform actions outside their desired functionality for process control.	In the 2015 attacks on the Ukrainian power grid, attackers issued unauthorized commands to open the breakers at substations that three regional electricity utilities managed, causing a loss of power to about 225,000 customers.[b]
Disruption to physical operating components	Malicious attackers can cause disruptions in infrastructure, equipment, and the surrounding environment when attacking industrial control systems. This technique may result in a breakdown in industrial control systems devices or represent tangential damage from other techniques used in an attack.	In December 2014, a cyberattack resulted in the misoperation of an industrial control system, including the improper shutdown of a furnace and physical damage to a German steel mill's facilities.[c]
Loss of productivity and revenue	Attackers may cause loss of productivity and revenue through disruption and even damage to the availability and integrity of industrial control systems operations, devices, and related processes.	In December 2019, a form of ransomware, named EKANS, infected various industrial control systems devices, reportedly in the U.S., Europe, and Japan, by encrypting files and displaying a ransom note, which impaired operations.[d]
Loss of visibility	Distribution utilities lose visibility into operations of the grid, allowing the attacker to hide the present state of system operations. This can occur without affecting the physical distribution systems processes themselves.	In March 2019, an attacker exploited known vulnerabilities in an internet-connected firewall to cause the firewall to reboot for approximately 5 minutes over a 10-hour period. As a result, an electric utility serving parts of California, Utah, and Wyoming experienced a communications outage between the control center and remote sites and equipment. This created a denial of service condition, which prevents utility staff from monitoring and controlling the system.[e]

Source: GAO analysis and summary of relevant documents. | GAO-21-81

[a]These tactics to affect distribution systems are not mutually exclusive. Some tactics may be used in conjunction with one another.

[b]SANS Industrial Control Systems, Analysis of the Cyber Attack on the Ukrainian Power Grid (North Bethesda, MD.: Mar. 18, 2016).

[c]SANS Industrial Control Systems, ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack (Rockville, MD.: Dec. 30, 2014).

[d]Dragos, EKANS Ransomware and ICS Operations, accessed November 25, 2020, https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/.

[e]North American Electric Reliability Corporation, Risks Posed by Firewall Firmware Vulnerabilities (Atlanta, GA.: Sept. 4, 2019).

GPS

The grid's distribution systems increasingly depend on GPS for precise timing information to monitor and control their functions. For example, phasor measurement units—devices used to measure the voltage or current in the electricity grid—rely on GPS to synchronize real-time measurements among multiple devices. Officials we interviewed from two national laboratories highlighted that such devices are increasingly used in the grid's distribution systems.

Disturbances in GPS signals that phasor measurement units receive could limit visibility into system operations, which could result in unsynchronized measurements that could cause misoperation of equipment and power outages. In particular, GPS is susceptible to exploitation by malicious actors through jamming or spoofing, which attacks the availability or integrity of GPS, respectively. GPS jamming is the transmission of radio frequency signals that intentionally interfere with or block valid GPS signals. Additionally, a malicious actor could transmit a false GPS signal—known as GPS spoofing—that could deceive a receiver into reporting an incorrect time or location.

Networked Consumer Devices and Distributed Energy Resources

A growing number of consumers are using networked consumer devices that are connected to the grid's distribution systems, such as electric vehicles and charging stations, and smart inverters.[38] These devices can be high wattage, which means they can demand a high amount of electricity from the grid. However, distribution utilities have limited visibility and influence on the use and cybersecurity of these devices because consumers typically control them, according to officials from a national laboratory.

Federal and nonfederal entities we interviewed said that networked consumer devices connected to the grid's distribution systems potentially introduce vulnerabilities. These views are consistent with findings in our previous work. In particular, we have previously reported that networked consumer devices are vulnerable to cyberattacks, including those involving malware that attackers could leverage in a cyberattack impacting the grid.[39] Additionally, we reported that in 2018, university researchers found that malicious threat actors could compromise a large number of high-wattage networked consumer devices (e.g., smart water heaters) and turn them into a botnet.[40] The malicious actors could then use the botnet to launch a coordinated attack aimed at increasing or decreasing the electricity demands across distribution systems to disrupt grid operations (see fig. 3).[41] According to officials we interviewed from

[38]A smart inverter is a device that converts electrical currents from solar panels to be used by consumers in their homes. This type of inverter allows for regulating voltages and other grid support functions not usually found in legacy inverters.

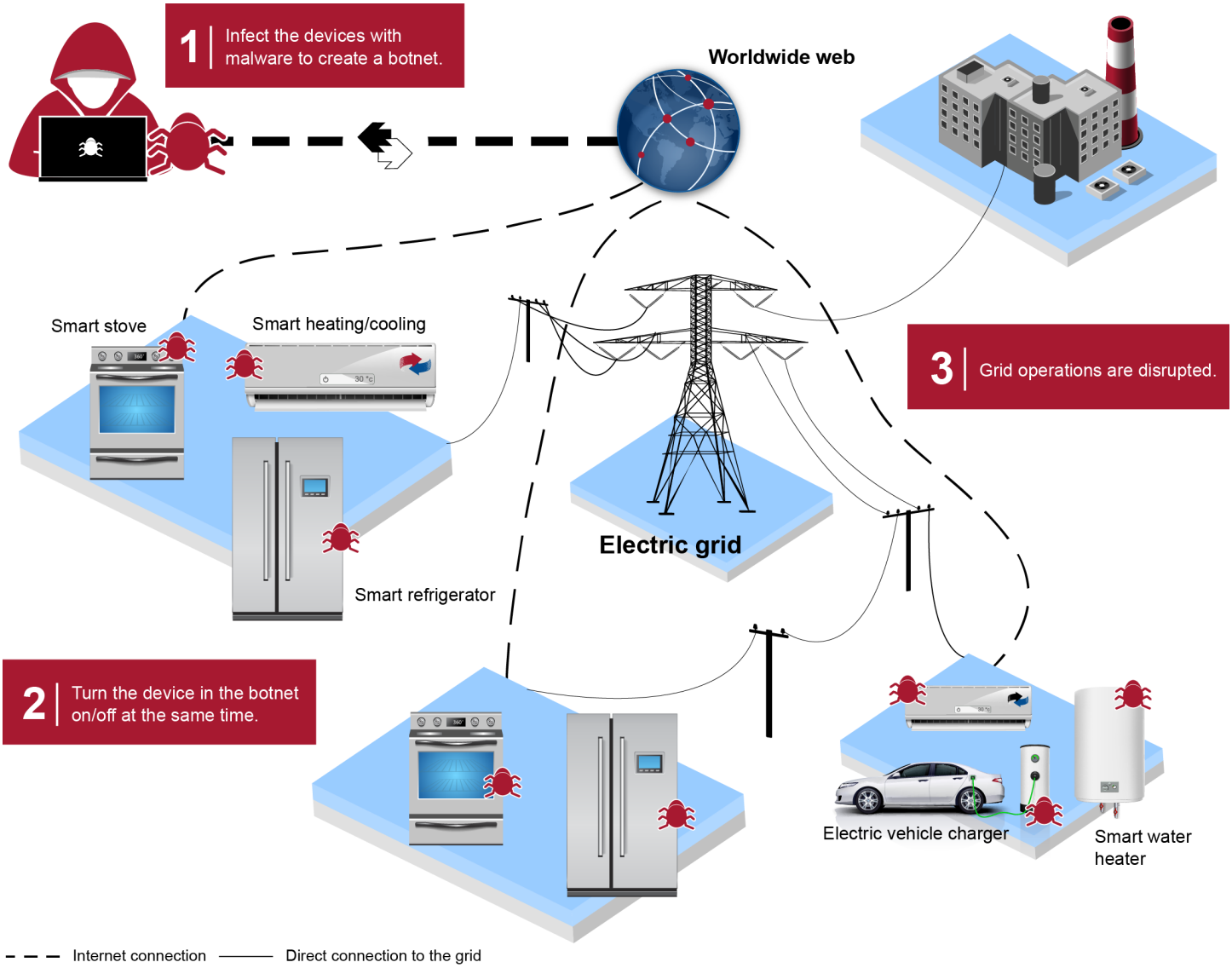
[39]GAO, *Internet of Things: Status and Implications of an Increasingly Connected World,* GAO-17-75 (Washington D.C.: May 15, 2017).

[40]GAO-19-332.

[41]A botnet is a network of devices infected with malicious software and controlled as a group without the owners' knowledge.

national laboratories, the likelihood of such an attack is currently low, but the growing usage of networked consumer devices on the grid's distribution systems could increase this vulnerability.

Figure 3: Example of an Attacker Compromising High-Wattage Networked Consumer Devices



Sources: GAO and university research; images left to right: ifh85/stock.adobe.com, sveta/stock.adobe.com, and mark.f/stock.adobe.com. | GAO-21-81

In addition, distributed energy resources are increasingly connected to the grid's distribution systems and may be leveraged in a cyberattack.[42] These devices can include rooftop solar units and battery storage units. When connected to the grid's distribution systems, such devices may introduce vulnerabilities, according to federal officials we interviewed. According to officials at one national laboratory, distributed energy resources can make distribution systems more vulnerable because of their distributed nature, their control and communication requirements, and the larger number of devices and access points operating outside utilities' control. For example, companies that offer residential solar energy products can retain the capability to remotely monitor and manage the units. In 2015, a solar energy company remotely updated the software of 800,000 of its customers' smart solar inverters through the company's networks.[43] However, a national laboratory found that such remote access poses a vulnerability.[44] Specifically, an attacker may be able to compromise the company's access to these devices to instruct them to perform actions outside their desired functionality, which could result in disruptions to the grid's distribution systems operations. For instance, an attacker may instruct compromised solar inverters to inject power into the grid to cause voltage and stability issues, potentially resulting in a power outage.

Various Threat Actors Are Capable of Carrying Out a Cyberattack on Grid Distribution Systems

Various threat actors are increasingly capable of carrying out a cyberattack on the grid's distribution systems, according to all of the national laboratory officials we interviewed. Nations, criminal groups, terrorists, hackers and hacktivists, and insiders pose threats to the bulk power system.[45] Further, the *2019 Worldwide Threat Assessment of the U.S. Intelligence Community* and the *2020 Homeland Threat Assessment* note that nations and criminal groups pose the greatest cyberattack threats to critical infrastructure.[46] According to federal officials we

[42]Distributed energy resources are any resource on distribution systems that produces electricity and is not included in the bulk power system.

[43]Solar inverters regulate the voltage of power being generated by solar panels and fed into the grid.

[44]Sandia National Laboratories, *Cyber Security Assessment of Distributed Energy* Resources, (Albuquerque, NM: June 2017).

[45]GAO-19-332.

[46]The *2019 Worldwide Threat Assessment of the U.S. Intelligence Community* notes the cyber risk of terror organizations, in addition to nations and criminal groups. However, the more recent *2020 Homeland Threat Assessment* does not identify terrorists as one of the top cyber threats facing the nation's critical infrastructure.

interviewed, these threat actors may also pose a threat to the grid's distribution systems (see table 3). In addition, these officials stated that terrorists, hackers/hacktivists, and insiders also pose a threat to the grid's distribution system.

Table 3: Threat Actors That May Pose Significant Threats to the Grid's Distribution Systems

Threat actor	Description
Nations	Nations, including groups or programs sponsored or sanctioned by nation states, use cyber tools as part of their information-gathering and espionage activities. According to the 2019 Worldwide *Threat Assessment of the U.S. Intelligence Community* and the 2020 *Homeland Threat Assessment*, China and Russia pose the greatest cyberattack threats;[a] of particular concern, they have the ability to launch cyberattacks that could disrupt or damage critical infrastructure.[b]
Criminal groups	Criminal groups, including organized crime organizations, seek to use cyberattacks for monetary gain. According to the *2020 Homeland Threat Assessment*, cybercriminals increasingly will target critical infrastructure to generate profit. That assessment also states that criminal organizations often use ransomware—malicious software used to deny access to systems or data—against critical infrastructure entities at the state and local levels by exploiting gaps in cybersecurity.[c]
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, inflict mass casualties, weaken the economy, and damage public morale and confidence. However, while terrorists are highly motivated, they do not currently have the sophisticated tools or skill necessary to execute a cyberattack that could cause a widespread outage or significantly damage the power system, according to the *2019 Worldwide Threat Assessment*. Nonetheless, terrorists could create disruptions, such as by executing denial-of-service attacks against poorly protected networks.
Hackers and hacktivists	Hackers break into networks for a challenge, revenge, stalking, or monetary gain, among other reasons. By contrast, hacktivists are ideologically motivated and use cyber exploits to further political goals, such as free speech or making a point. Hackers and hacktivists no longer need a great amount of skill to compromise information technology (IT) systems because they can download commonly available cyberattack tools. Hackers and hacktivists may have less capability to do harm than nations,[d] but their intent to inflict harm or to damage operations is typically more immediate than nations' longer-term goals.
Insiders	Insiders are individuals (e.g., employees, contractors, vendors) with authorized access to an information system or enterprise who have the potential to cause harm, wittingly or unwittingly, through destruction, disclosure, or modification of data or through denial of service. Insiders could include knowledgeable employees with privileged access to critical systems or contractors with limited system knowledge.

Sources: Summary of GAO, Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid, GAO-19-332 (Washington, D.C.: Aug. 26, 2019), and relevant federal documents. | GAO-21-81

[a]The assessment also states that Iran is attempting to deploy cyberattack capabilities that would enable attacks against critical infrastructure and that North Korea retains the ability to conduct disruptive cyberattacks.

[b]According to the Department of Justice, the December 2015 Ukrainian blackout was caused by nation-sponsored cyberattacks on regional distribution companies. In October 2020, the Department of Justice charged six Russian intelligence officers in relation to those cyberattacks.

[c]According to the Department of Homeland Security, ransomware continues to be a major threat to both IT and industrial control systems that support the grid.

[d]GAO, Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid, GAO-19-332 (Washington, D.C.: Aug. 26, 2019).

The Scale of Potential Cyberattack Impacts on Grid Distribution Systems Is Unclear

None of the cybersecurity incidents reported in the United States have disrupted the reliability or availability of the grid's distribution systems, according to DOE, which requires all U.S. electric utilities to report significant electrical incidents or disturbances. However, cyberattacks on foreign grid distribution systems have resulted in localized power outages, such as the 2015 blackout in Ukraine.[47]

According to three federal and nonfederal entities we interviewed, the impacts of cyberattacks on the grid's distribution systems are likely to be localized. For example, officials from one national laboratory noted that any cyberattacks capable of disrupting power on the grid's distribution systems would likely only disrupt the electricity distributed locally from any affected substations; an attack would have to be coordinated with another event to cause widespread effects. However, these statements were generally based on the professional experience of the federal and nonfederal entities we interviewed, and none of them were aware of any assessments confirming that cyberattacks on distribution systems would result in only localized impacts. Moreover, three federal and national laboratory officials told us that even if a cyberattack on the grid's distribution systems was localized, such an attack could still have significant national consequences, depending on the specific distribution systems that were targeted and the severity of the attack's effects. For instance, an attack on the grid's distribution systems for a large city could result in outages of national significance.

Further, officials from another national laboratory said the extent to which the bulk power system is susceptible to disruption from attacks on distribution systems is unclear. For instance, they told us that the scale of potential impacts on the bulk power system from a cyberattack on the grid's distribution systems is not well understood.

[47]In October 2020, the Department of Justice charged six Russian intelligence officers in relation to those cyberattacks.

Selected States and Industry Have Taken Varied Actions Aimed at Improving Grid Distribution Systems' Cybersecurity

Selected states and industry have taken various actions aimed at improving the cybersecurity of the grid's distribution systems, including hiring dedicated cybersecurity personnel and assessing their cybersecurity posture, but those actions are not uniform across jurisdictions. Federal agencies have supported state and industry actions by, for example, providing cybersecurity training and guidance.

Selected State and Industry Actions Intended to Improve Distribution Systems' Cybersecurity Vary

Selected State Actions

Selected states have all incorporated cybersecurity into their oversight responsibilities, and half hired cybersecurity personnel to help improve the cybersecurity of their distribution systems.

- **Oversight responsibilities.** Officials from all six state public utility commissions we interviewed said they do not have mandatory cybersecurity standards for the grid distribution systems within their jurisdiction, but they all told us they have incorporated cybersecurity into their routine oversight responsibilities. For example, officials from three of the commissions told us their oversight responsibilities include periodic meetings with utilities, during which they discuss the utilities' cybersecurity programs and plans. One of these commissions also stated that they provide utilities with a risk assessment program that includes an examination of their cybersecurity posture, which the utilities use to inform their rate justification.

  The other three commissions take varying approaches to incorporating cybersecurity into their oversight responsibilities. For instance, officials from one commission told us their state legislature recently passed legislation giving the commission more authority to ensure that utilities throughout the state employ cybersecurity best practices. Officials from another commission told us the commission performs a management audit of utilities and incorporates cybersecurity into that process. The other commission's officials said the commission has used its broad regulatory authority to review utilities' response to incidents.

- **Cybersecurity personnel.** Officials from three of the six state public utility commissions we interviewed said their commission had hired dedicated personnel with cybersecurity responsibilities. Specifically, officials from one commission said the commission hired a director in 2018 and has a committee comprising staff from the commission's various regulatory offices to manage the organization's oversight of utility cybersecurity. Another commission created a new internal cybersecurity position responsible for oversight of certain utilities that are not subject to FERC-approved reliability standards. Similarly, an official from a third commission told us their public utility commission hired staff to set up a cyber-policy unit within the commission, which would develop appropriate guidelines for utilities on the state's distribution systems. However, officials from two other commissions we interviewed said they do not have resources to hire dedicated personnel with cybersecurity expertise, and officials from another commission said they rely on the utility to manage their cybersecurity.

Selected Industry Actions

Selected distribution utilities have taken various actions intended to improve their cybersecurity, including incorporating cybersecurity into their internal practices and processes and assessing their cybersecurity posture. Representatives from all six of the distribution utilities we interviewed told us that they are not subject to any mandatory standards specific to cybersecurity, but each has incorporated cybersecurity into their internal practices. For example, a representative of one utility told us their utility had incorporated cybersecurity into their governance structure to improve cybersecurity for both its transmission and distribution assets. Representatives of another utility we interviewed told us they recently incorporated new formal processes for managing cybersecurity efforts across their organization. They added that activities they conduct include tabletop exercises and working with universities to develop courses on grid cybersecurity for their staff.

In addition, representatives of all six distribution utilities we interviewed reported using DOE's Cybersecurity Capability Maturity Model and other tools to assess their cybersecurity posture and manage cybersecurity risks.[48] Representatives of one utility stated they have used both DOE's Cybersecurity Capability Maturity Model and the American Public Power

[48]DOE's Cybersecurity Capability Maturity Model can be used to inform the development of a new cybersecurity program and focuses on the implementation and management of cybersecurity practices associated with the IT and industrial control systems assets and the environments in which they operate.

Association's cybersecurity scorecard self-assessment as part of their efforts to monitor and improve their cybersecurity posture.[49] Another utility we interviewed told us they have identified free opportunities to bolster their cybersecurity efforts, such as the National Rural Electric Cooperative Association's Rural Cooperative Cybersecurity Capabilities program and DHS's cyber assessment services.[50] Representatives of another utility told us they use the NIST Cybersecurity Framework and NIST standards to inform how they conduct their assessments.[51]

Industry associations we spoke with have also provided resources to states and distribution utilities to assist in their cybersecurity practices. For example, the National Association of Regulatory Utility Commissioners provides state public utility commissions with resources, such as its *Cybersecurity Strategy Development Guide and Understanding Cybersecurity Preparedness: Questions for Utilities*, to help commissions engage with utilities and evaluate their cybersecurity risk management practices.[52] National Rural Electric Cooperative Association representatives told us they were working with DOE and a national laboratory to provide a self-assessment tool and free or low-cost trainings to its membership of cooperative utilities. Further, representatives of the American Public Power Association told us their outreach efforts to its member utilities have included webinars, conferences, and coordination with DOE to develop more products that utilities could use to assess their cybersecurity. In addition, the Electricity Information Sharing and Analysis Center shares threat intelligence information quickly to industry and federal agencies, and it provides

[49]The American Public Power Association's Public Power Cybersecurity Scorecard is an online self-assessment tool for public power utilities to assess cyber risk, plan improvements, prioritize investments, and benchmark their cybersecurity posture.

[50]The National Rural Electric Cooperative Association's *Rural Cooperative Cybersecurity Capabilities* program focuses on developing tools and resources for improving cybersecurity capabilities of electric cooperatives. The program provides electric cooperatives with self-assessment tools, education and networking opportunities, and resources and guides to assist them in improving their cybersecurity posture. DHS provides various cyber resources for utilities, among other critical infrastructure operators, including risk and vulnerability assessments, cyber resilience reviews, and vulnerability scanning.

[51]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Washington, D.C.: April 2018).

[52]National Association of Regulatory Utility Commissions, *Cybersecurity Strategy Development Guide* (Washington, DC: October 2018); and *Understanding Cybersecurity Preparedness: Questions for Utilities* (Washington, D.C.: June 2019).

member utilities with a central channel to escalate physical security and cybersecurity issues. It also provides members access to cybersecurity services, such as malware reverse engineering.

Federal Agencies Have Provided Support to States and Industry to Help Improve Distribution Systems' Cybersecurity

Federal agencies have provided support to states and industry to help improve the cybersecurity of the grid's distribution systems. This support includes

- **Training and exercises.** Federal agencies provide distribution utilities with various training and exercise opportunities to assist them in managing their cybersecurity. For example, the North American Electric Reliability Corporation (NERC) partners with DOE every other year to conduct GridEx—a large, geographically distributed grid security exercise. In this exercise, industry representatives (including from distribution utilities) and government officials execute an emergency response to simulated cyber and physical security threats and incidents.[53] Representatives of four distribution utilities we interviewed stated that they have participated in GridEx to improve their cyber posture. In addition, DHS offers various cybersecurity training to the electricity sector, including distribution utilities. The training covers areas such as workforce development, industrial control systems, and physical security.
- **Assessment tools.** DOE and DHS provide distribution utilities and the rest of the electric power industry with tools to assess their cybersecurity posture and maturity level. For example, DOE offers its Cybersecurity Capability Maturity Model to help utilities assess their cybersecurity maturity, as previously mentioned.[54] Representatives from the National Rural Electric Cooperative Association told us that they used DOE's Cybersecurity Capability Maturity Model to inform the cybersecurity assessment tool that they created specifically for their members. DHS also provides free cybersecurity assessment services, such as vulnerability scanning and remote penetration testing, to critical infrastructure organizations, including utilities.
- **Guidance and best practices.** NIST has developed several publications on cybersecurity protections and best practices for the

[53]NERC is the federally designated U.S. electric reliability organization responsible for conducting reliability assessments and developing and enforcing mandatory standards to provide for reliable operation of the bulk power system, which FERC oversees.

[54]Additionally, in September 2020, DOE announced a cooperative agreement that grants the American Public Power Association and National Rural Electric Cooperative Association $6 million each to develop cybersecurity tools for distribution utilities by 2023.

electricity sector.[55] Representatives from three distribution utilities we interviewed told us they use the NIST Cybersecurity Framework to inform their cybersecurity practices. Further, DHS has released best practice guides that provide actions that can be taken to enhance the resiliency of position, navigation, and timing services like GPS.[56] Similarly, the North American SynchoPhasor Initiative, which DOE funds, has provided information related to increasing the effective use of synchophasor technology on the grid.[57] In addition, FERC has approved cybersecurity reliability standards for the bulk power system, which do not apply to the grid's distribution systems, but some utilities we interviewed said they voluntarily apply the standards to their distribution systems or use them as best practices. Representatives from one utility we spoke with said they voluntarily share details regarding cybersecurity incidents impacting their organization with DOE.

- **Threat information.** DOE has programs focused on sharing cybersecurity threat information with the electricity sector, including the Cyber Risk Information Sharing Program—a voluntary, bi-directional, public-private IT data-sharing and analysis platform—and provides monthly threat briefings to the electricity sector through the Electricity Information Sharing and Analysis Center, which NERC operates. A representative from one utility we spoke with said their company participates in the Cyber Risk Information Sharing Program

[55]For example, National Institute of Standards and Technology*, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0,* NIST SP 1108r4 (Washington, D.C.: February 2021); *Energy Sector Asset Management for Electric Utilities, Oil & Gas Industry,* NIST SP 1800-23 (Washington, D.C.: May 2020); *Situational Awareness for Electric Utilities,* NIST SP 1800-7 (Washington, D.C.: August 2019); *Cybersecurity Framework Smart Grid Profile*, NIST Technical Note 2051 (Washington, D.C.: July 2019); *Identity and Access Management for Electric Utilities*, NIST SP 1800-2 (Washington, D.C.: July 2018); *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1 (Washington, D.C.: April 2018); and *Guidelines for Smart Grid Cybersecurity*, NIST Interagency Report (NISTIR) - 7628 Rev. 1 (Washington, D.C.: September 2014).

[56]Department of Homeland Security, *Resilient Position, Navigation, and Timing (PNT) Conformance Framework*, Version 1.0 (Washington, D.C.: August 2020); *Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations* (Washington, D.C.: January 2015); and *Improving the Operation and Development of Global Positioning System Equipment Used by Critical Infrastructure* (Washington, D.C.: January 2017).

[57]For example, the North American SynchoPhasor Initiative issued a report on the effective application of synchophasor technology in distribution systems. North American SynchoPhasor Initiative, *Synchronized Measurements and their Applications in Distribution Systems: An Update*, NASPI-2020-TR-016 (June 2020).

as part of its efforts to improve its cyber posture, but representatives from the National Rural Electric Cooperative Association said the program is too expensive for some of its members. Additionally, DHS officials said they provide vulnerability information to electricity stakeholders and recommend specific mitigations to address identified vulnerabilities. DHS also provides security clearances to private sector entities through its Private Sector Clearance Program for Critical Infrastructure so they can access classified information to make more informed decisions.[58]

- **Research and development.** DOE has funded research and development projects at national laboratories to help improve the cybersecurity of the grid's distribution systems. Examples of such projects are shown in table 4.

[58]The Private Sector Clearance Program for Critical Infrastructure, established in 2006, ensures that critical infrastructure private-sector owners, operators, and industry representatives, specifically those in positions responsible for the protection, security, and resilience of their assets, are processed for the appropriate security clearances. With clearances, these owners, operators, and representatives can access classified information to make more informed decisions. The program facilitates the processing of these security clearance applications for private-sector partners.

Table 4: Examples of National Laboratory Research and Development Projects for Electricity Grid Distribution Systems

Project lead	Project title	Description
Brookhaven National Laboratory	Assess the Impact and Evaluate the Response to Cybersecurity Issues	Aims to build a user-friendly tool to assess the impact and evaluate the response to cybersecurity issues on forecasting data used to operate energy delivery systems.
Idaho National Laboratory	Cybersecurity for the Operational Technology Environment	Aims to determine what data to collect and how to securely share sensitive operational data for enhanced analysis—all the while protecting privacy and meeting cybersecurity regulations.
	Cyber Testing for Resilient Industrial Control Systems	Seeks to measure and address digital supply chain security vulnerabilities due to the use of common subcomponents in industrial control systems devices.
Lawrence Livermore National Laboratory	Cybersecure Interconnection of Distributed Energy Resources Analysis	Aims to develop a tool that can evaluate the cybersecurity risk of various distributed energy resource integration architectures and design remediation strategies so that a grid with a large number of distributed energy resources can become more resilient and be better able to survive a cyberattack.
National Renewable Energy Laboratory	Cyber Energy Emulation Platform	Aims to build a cyber energy emulation platform for energy system environments that allows researchers to explore the potential consequences of a cybersecurity threat, analyze its impact on the power system, and identify mitigation response strategies.
	Advanced Research on Integrated Energy Systems	Research platform that involves visualization, monitoring, and data processing for research assets and the connections between them. The platform has the ability to simulate and detect cyber attacks on communications and control systems that are still evolving, with an effect of reducing overall vulnerabilities in energy systems.

Source: GAO summary of national laboratory and Department of Energy documents and interviews. | GAO-21-81

DOE Has Not Fully Addressed Risks to Grid Distribution Systems from Cyberattacks in Its Plans

Under federal policy, DOE is responsible for implementing the energy sector portion of the national cybersecurity strategy for critical infrastructure, including developing and coordinating a plan for addressing grid cybersecurity.[59] National strategies are critical tools to help address long-standing and emerging issues that affect national

[59]DOE has this responsibility as the designated sector-specific agency for the energy sector under Presidential Policy Directive 21. Under the National Defense Authorization Act for Fiscal Year 2021, DOE—as the Sector Risk Management Agency for the energy sector—is also responsible for supporting energy sector risk management, including identifying, assessing, and prioritizing risks. In addition, DHS is responsible for coordinating with DOE on the development of a national plan to address cybersecurity risks facing the grid under the directive.

security and economic stability.[60] It is important for these strategies to describe the steps that are necessary to fully address these long-standing and emerging issues, including risks, in order to ensure they are useful in resource and policy decisions.[61] In line with its responsibility, DOE has led the development of three plans and an assessment that, together, represent the department's efforts to implement the national cybersecurity strategy for the energy sector, including the grid's distribution systems.[62]

Collectively, DOE's plans and assessment address some elements of risks that enable cyberattacks on the grid's distribution systems, such as vulnerabilities that enable cyberattacks on industrial control systems. For example, DOE's *Multiyear Plan for Energy Sector Cybersecurity* describes plans to enhance threat analysis capabilities that will enable smarter, more targeted, and informed monitoring of critical industrial control systems networks. Specifically, DOE plans to expand the capabilities of its Cyber Risk Information Sharing Program—which currently only provides information related to IT networks—to also monitor, analyze, and share threat indicators for operational networks that are similarly vulnerable. However, the plans and assessment do not address other vulnerabilities associated with industrial control systems or vulnerabilities related to supply chain, GPS-dependent devices, and networked consumer devices not controlled by distribution utilities. For instance, they do not address vulnerabilities related to solar inverters and electric vehicle chargers.

In August 2019, we found that DOE's plans and assessment to implement the energy sector portion of the national cybersecurity strategy for critical infrastructure did not fully address the key characteristics of a national

[60]As previously mentioned, the executive branch has taken steps toward outlining a national strategy for confronting cyber threats to the grid. For example, in February 2020, the White House issued Executive Order 13905, which is designed to ensure that the disruption or manipulation of positioning, navigation, and timing services—like GPS—does not undermine the reliable and efficient functioning of critical infrastructure, including the grid.

[61]GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[62]Department of Energy and Department of Homeland Security, *Energy Sector-Specific Plan, 2015;* and *Assessment of Electricity Disruption Incident Response Capabilities.* Department of Energy, *Multiyear Plan for Energy Sector Cybersecurity;* and *EERE Cybersecurity Multiyear Program Plan.*

strategy.[63] We recommended that DOE develop a plan that addressed the key characteristics of a national strategy, including a full assessment of cybersecurity risks to the grid. DOE officials told us they are working to update their plans in response to our recommendation. However, officials noted that the updated versions will continue to address the cybersecurity risks to the grid's distribution systems to the same extent as the previous plans and assessment, which did not fully address risks to distribution systems. For example, in October 2020, DOE issued a plan to support its *Multiyear Plan for Energy Sector Cybersecurity*, but the plan does not fully address the elements of risks to the grid's distribution systems, including vulnerabilities associated with internet-accessible industrial control systems devices and networked consumer devices.[64]

DOE officials told us that they are not addressing risks to grid distribution systems to a greater extent in their updated plans because they have prioritized addressing risks facing the bulk power system. Officials said a cyberattack on the bulk power system would likely affect large groups of people very quickly, and the impact of a cyberattack on distribution systems would likely be less significant.

However, as previously mentioned, none of the federal and nonfederal entities that we spoke with were aware of any assessments confirming the scale of potential impacts of a cyberattack on distribution systems. In addition, even if a cyberattack on the grid's distribution systems did not impact the bulk power system, such an attack could still have significant national consequences, depending on the specific distribution systems that were targeted and the severity of the attack's effects, according to some federal and nonfederal officials we interviewed. For instance, an attack on the grid's distribution systems for a large city could result in outages of national significance, according to officials from a cybersecurity firm. Additionally, a coordinated attack on distribution systems could cause outages in multiple areas even if it did not disrupt the bulk power system, according to officials from one national laboratory.

Unless DOE more fully addresses risks to the grid's distribution systems from cyberattacks, including their potential impacts, in its plans to implement the national cybersecurity strategy for the grid, the updated

[63]See GAO-19-332. Key characteristics of a national strategy include an analysis of the threats to and vulnerabilities of critical assets and operations.

[64]Department of Energy, *EERE Cybersecurity Multiyear Program Plan.*

documents will likely be of limited use in prioritizing federal support to help states and industry improve grid distribution systems' cybersecurity.

Conclusions

The grid's distribution systems, which carry to consumers the electricity essential to modern life, are increasingly at risk from cyberattacks. DOE, DHS, and other federal agencies have provided resources to states and industry to help them improve the cybersecurity of distribution systems. However, DOE's plans for implementing the national cybersecurity strategy for the grid do not fully address risks to these systems. While a cyberattack on distribution systems may be less significant than one on the bulk power system, the impacts of such an attack could still result in outages of national significance. Unless DOE more fully addresses risks to the grid's distribution systems in its updated plans, federal support intended to help states and industry improve distribution systems' cybersecurity will likely not be effectively prioritized.

Recommendation for Executive Action

The Secretary of Energy, in coordination with DHS, states, and industry, should more fully address risks to the grid's distribution systems from cyberattacks—including the potential impact of such attacks—in DOE's plans to implement the national cybersecurity strategy for the grid. (Recommendation 1)

Agency Comments

We provided a draft of this report for review and comment to DOE—the agency to which we made a recommendation—as well as DHS, FERC, and the Department of Commerce (on behalf of NIST). In its comments, reproduced in Appendix II, DOE agreed with our recommendation and highlighted two research projects with the goal of advancing the cybersecurity of distribution systems. These research projects may help states and industry improve the cybersecurity of distribution systems, but it will also be important for DOE to more fully address risks to the grid's distribution systems from cyberattacks in DOE's plans to implement the national cybersecurity strategy for the grid.

DOE, DHS, FERC, and the Department of Commerce also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the Secretaries of Commerce, Energy, and Homeland Security, and the Chairman of FERC. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff members have any questions about this report, please contact Frank Rusco at (202) 512-3841 or ruscof@gao.gov, and Nick

Marinos at (202) 512-9342 or marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Frank Rusco
Director, Natural Resources and Environment

Nick Marinos
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the extent to which the grid's distribution systems are at risk from cyberattacks and the scale of potential impacts from such attacks, (2) describe selected state and industry actions to improve distribution systems' cybersecurity and federal efforts to support those actions, and (3) examine the extent to which DOE has addressed risks to grid distribution systems from cyberattacks in its plans for implementing the national cybersecurity strategy for the energy sector.

To address the first two objectives, we conducted semistructured interviews with officials and representatives from 38 key federal and nonfederal entities that play a role in grid distribution systems' cybersecurity. Specifically, we interviewed officials or representatives from the following:

Federal entities

- We interviewed officials from four federal agencies with responsibilities related to distribution systems' cybersecurity—the Department of Energy (DOE), the Department of Homeland Security (DHS), the Federal Energy Regulatory Commission (FERC), and the National Institute of Standards and Technology (NIST).
- We also interviewed officials from the following nine national laboratories: Argonne, Brookhaven, Idaho, Lawrence Livermore, National Renewable Energy, Oak Ridge, Pacific Northwest, Sandia, and Savannah River. We selected these national laboratories because they had previous or ongoing research and development projects related to grid distribution systems' cybersecurity, were identified from previous GAO reports, or because federal agency officials recommended them.

Nonfederal entities

State Officials

- We interviewed officials from six state public utility commissions—the California Public Utilities Commission, Georgia Public Service Commission, Pennsylvania Public Utility Commission, Texas Public Utility Commission, Vermont Department of Public Services, and Washington Utilities and Transportation Commission. To select these commissions, we used three primary criteria: (1) commissions in states that contained the three utility types (investor-owned, publicly owned, and cooperative), (2)

commissions in states representing each of the three interconnections (Eastern, Western, and Electric Reliability Council of Texas), and (3) recommendations from entities we interviewed.

Industry Representatives

- We interviewed representatives from six distribution utility companies, including two investor-owned utilities, three publicly owned utilities, and one cooperative. To select these utilities, we used three primary criteria: (1) distribution utilities within the states of selected public utility commissions, (2) utilities that support a relatively large customer base compared with similar utility types in the state, and (3) utilities that are part of parent companies that were identified on DHS's Section 9 list of critical infrastructure.[1]
- We interviewed representatives from seven electric industry associations, including the American Public Power Association, Edison Electric Institute, Electricity Information Sharing and Analysis Center, National Rural Electric Cooperative Association, National Association of Regulatory Utility Commissioners, National Association of State Energy Officials, and National Electrical Manufacturers Association. We selected these electric industry associations because of their relevant knowledge of the cybersecurity of grid distribution systems, and we identified these electric industry associations from previous GAO reports and stakeholder recommendations.
- We interviewed representatives from two cybersecurity firms, which we selected because of their relevant knowledge of the cybersecurity of grid distribution systems and identified through recommendations from entities we interviewed.
- We interviewed representatives from three grid equipment manufacturers, which we selected because of their relevant knowledge of the cybersecurity of grid distribution systems and identified through recommendations from entities we interviewed.

[1]DHS annually identifies and maintains a list of critical infrastructure entities that meet the criteria specified in Executive Order 13636, Improving Critical Infrastructure Cybersecurity, Section 9(a). Section 9 entities are defined as critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

- We interviewed one industry researcher, whom we selected because of their relevant knowledge of the cybersecurity of grid distribution systems and identified from previous GAO reports and recommendations from entities we interviewed.

We conducted a content analysis of these entities' responses to identify any themes related to managing grid distribution systems' cybersecurity risks. The views of the officials and representatives we interviewed cannot be generalized but provide valuable insight into the extent to which the grid's distribution systems are at risk from cyberattacks, and actions intended to improve distribution systems' cybersecurity.

To describe the extent to which the grid's distribution systems are at risk from cyberattacks and the scale of potential impacts from such attacks, we identified vulnerable components and processes that could be exploited, developed a list of actors that could pose a threat to distribution systems, and reviewed the potential impact of cyberattacks on distribution systems. Specifically, to identify grid distribution systems' cybersecurity vulnerabilities, we reviewed the MITRE ATT&CK® for Industrial Control Systems framework[2] and our prior work on grid cybersecurity.[3] We also interviewed key federal and nonfederal entities to identify potential vulnerabilities and any related reports or assessments. To develop the list of threat actors, we reviewed our prior work,[4] the Office of the Director of National Intelligence's Worldwide Threat Assessment,[5] and other relevant

[2]MITRE Corporation, Main Page, "ATT&CK® for Industrial Control Systems," last modified on June 3, 2020, https://collaborate.mitre.org/attackics/index.php/Main_Page. The MITRE Corporation is a not-for-profit organization that conducts research and development in areas such as cyber threat sharing and cyber resilience. The MITRE Corporation also operates several federally funded research and development centers, including the National Cybersecurity Center of Excellence and the Homeland Security Systems Engineering and Development Institute.

[3]GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 17, 2019).

[4]GAO-19-332 and *Cybersecurity: Challenges in Securing the Electric Grid,* GAO-12-926T (Washington, D.C.: July 17, 2012).

[5]Daniel R. Coats, Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, testimony before the Senate Select Committee on Intelligence, 116th Cong., 1st sess., January 29, 2019.

reports from DOE and DHS.[6] We also interviewed the key federal agencies listed previously to confirm, add, or remove threat actors based on their potential to execute attacks on grid distribution systems. To identify potential impacts of cyberattacks on grid distribution systems, we reviewed our prior work on grid cybersecurity[7] and nonfederal reports and assessments of cyberattacks on industrial control systems.[8] In addition, we interviewed the key federal and nonfederal entities listed previously to identify potential impacts of an attack on grid distribution systems and identify any related studies. We also interviewed relevant federal agencies and the North American Electric Reliability Corporation to determine whether any reported cybersecurity incidents affecting distribution systems have disrupted the reliability or availability of the grid.

To describe selected state and industry actions to improve grid distribution systems' cybersecurity, we reviewed relevant documentation received from state public utility commissions, distribution utilities, and industry associations and interviewed these entities to identify any actions taken to manage cybersecurity risks. To describe federal efforts to support state and industry actions, we reviewed documentation and interviewed relevant agency officials to identify such efforts.

To examine the extent to which DOE has addressed risks to grid distribution systems from cyberattacks in its plans for implementing the national cybersecurity strategy for the energy sector, we reviewed and

[6]Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Securing Industrial Control Systems: A Unified Initiative FY2019 – 2023* (Washington, D.C.: July 2020); and *2020 Homeland Threat Assessment* (Washington, D.C.: October 2020); Department of Energy, Office of Inspector General, *Audit Report: Federal Energy Regulatory Commission's Monitoring of Power Grid Cyber Security,* DOE/IG-0846 (Washington, D.C.: January 2011).

[7]GAO-19-332.

[8]SANS Industrial Control Systems*, Analysis of the Cyber Attack on the Ukrainian Power Grid* (Rockville, MD.: Mar. 18, 2016)*;* and *ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack* (Rockville, MD.: Dec. 30, 2014)*;* Dragos*, EKANS Ransomware and ICS Operations, accessed September 30, 2020,* https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/*;* and North American Electric Reliability Corporation, *Risks Posed by Firewall Firmware Vulnerabilities* (Atlanta, GA: Sept. 4, 2019).

analyzed DOE's plans and assessment[9] to implement the strategy and incorporated findings from our prior work that compared those plans and assessment with leading practices identified by GAO on key characteristics for a national strategy.[10] We also reviewed relevant documentation from federal agencies and national laboratories and interviewed relevant federal officials to identify such efforts.

We conducted this performance audit from September 2019 to March 2021, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives

[9]Department of Energy, *EERE Cybersecurity Multiyear Program Plan* (Washington, D.C.: October 2020); and *Multiyear Plan for Energy Sector Cybersecurity* (Washington, D.C.: May 2018); Department of Energy and Department of Homeland Security, *Assessment of Electricity Disruption Incident Response Capabilities* (Washington, D.C.: August 2017); and *Energy Sector-Specific Plan, 2015* (Washington, D.C.: 2015).

[10]GAO-19-332.

Appendix II: Comments from the Department of Energy

Department of Energy
Washington, DC 20585

March 2, 2021

Mr. Frank Rusco
Director
Natural Resources and Environment
U.S. Government Accountability Office
441 G Street N.W.
Washington, DC 20548

The U.S. Department of Energy (DOE or Department) appreciates the opportunity to provide a management response to the Government Accountability Office (GAO) draft report titled, *Electricity Grid Cybersecurity: DOE Needs to Ensure It Plans to Fully Address Risks to Distribution Systems, GAO-21-81SU.*

The draft report contained one recommendation to DOE; DOE concurs with the recommendation. DOE's full response to the recommendation is included in the Enclosure.

GAO should direct any questions to Ian Moore, Audit Coordinator for the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), at ian.moore@hq.doe.gov or by phone at 410-253-1792; or to Fowad Muneer, Deputy Assistant Secretary for Cybersecurity of Energy Delivery Systems (CEDS), CESER, at fowad.muneer@hq.doe.gov, or by phone at 202-586-5961.

Sincerely,

Patricia A. Hoffman

Digitally signed by Patricia A. Hoffman
Date: 2021.03.02 15:18:52 -05'00'

Patricia A. Hoffman
Acting Assistant Secretary for the
Office of Cybersecurity, Energy Security, and
Emergency Response and the Office of
Electricity

Enclosure

Management Response
GAO Draft Report: "Electricity Grid Cybersecurity: DOE Needs to Ensure It Plans to Fully Address Risks to Distribution Systems, GAO-21-81SU"

Response to Report Recommendations

Recommendation #1: The Secretary of Energy, in coordination with DHS, states, and industry, should more fully address risks to the grid's distribution systems from cyber-attacks—including the potential impact of such attacks—in DOE's plans to implement the national cybersecurity strategy for the grid.

DOE Response: Concur

DOE appreciates the report and recommendation from the Government Accountability Office (GAO) on distribution grid cybersecurity and continues active partner engagement as DOE works to improve cybersecurity for the energy sector in its role as the sector risk management agency (formerly sector specific agency) for Energy. Accordingly, the Department will continue to focus on mitigation of cybersecurity risks and evaluate the most critical risks to the energy sector.

DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) addresses cybersecurity in the energy sector through CESER's cyber research and development, information sharing, discovery, and coordination efforts. CESER's work addresses cybersecurity risk across the generation, transmission, and distribution systems.

Specifically, CESER manages an R&D portfolio that includes research partnerships led by industry, academia, and DOE national laboratories that are advancing distribution-level cybersecurity. Since 2016, DOE has been engaged in two congressionally directed projects with the National Rural Electric Cooperative Association (NRECA) and the American Public Power Association (APPA) directly in the area of distribution cybersecurity. These initiatives were reinvigorated in 2020 to better address distribution risks, and DOE issued new awards for the implementation of cybersecurity solutions on the distribution system of NRECA and APPA membership.

The major deliverables for the congressionally directed projects are:

- NRECA
  - Technical solution development - March 2022
  - Deployment to 55 Utility members - September 2023

- APPA
  - Technology Selection – April 2022
  - Deployment to ~12 Public Power Asset Owner/Operator members – June 2023

Estimated Completion Date: September 2023

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Frank Rusco, (202) 512-3841 or ruscof@gao.gov

Nick Marinos, (202) 512-9342 or marinosn@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Kaelin Kuhn (Assistant Director), David Marroni (Assistant Director), Andrew Moore (Analyst-in-Charge), Luqman Abdullah, Anna Bennett, Christopher Businsky, Jonathan Felbinger, Wil Gerard, Cindy Gilbert, Mike Gilmore, Lee Hinga, and Cynthia Norris made key contributions to this report.