

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

**Complaint of Michael Mabee)
Related to Critical Infrastructure)
Protection Reliability Standards)**

Docket No. EL20-46-000

COMPLAINT

Submitted to FERC on May 11, 2020

Introduction

I am a private citizen who conducts public interest research on the security of the electric grid because I recognize the absolutely vital role of this infrastructure in powering every one of the nation's 16 critical infrastructures and in undergirding not just the well-being but the very survival of our modern society.

I am filing this complaint under 16 U.S. Code § 824o(d)(5)¹ and 16 U.S. Code § 824o(e)(3)² because:

- 1) The mandatory Critical Infrastructure Protection (CIP) standard CIP-013-1 (Cyber Security Supply Chain Risk Management) does not comport with Presidential Executive Order 13920: Securing the United States Bulk-Power System³, and
- 2) The Federal Energy Regulatory Commission (FERC) has not ensured that mandatory CIP standards "fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework."

¹ "The Commission, upon its own motion *or upon complaint*, may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section." [Emphasis added.]

² "On its own motion *or upon complaint*, the Commission may order compliance with a reliability standard and may impose a penalty against a user or owner or operator of the bulk-power system if the Commission finds, after notice and opportunity for a hearing, that the user or owner or operator of the bulk-power system has engaged or is about to engage in any acts or practices that constitute or will constitute a violation of a reliability standard." [Emphasis added.]

³ Attached hereto as Exhibit A.

Request for Investigation

I request that the Commission issue a public notice of this Complaint pursuant to 18 CFR § 385.206(d), investigate this Complaint and issue an appropriate order to the Electric Reliability Organization (“ERO”) to correct deficiencies.

Background

On July 21, 2016 FERC issued Order No. 829, Revised Critical Infrastructure Protection Reliability Standards.⁴ In this order, FERC:

“directs the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.”

CIP-013-1 was developed by NERC and approved by FERC on October 26, 2018⁵ although the implementation date has been delayed.⁶ As of this filing, the standard has yet to be implemented – almost 4 years after FERC directed the standard.

Notwithstanding the bureaucratic delays and onerous process to develop a standard, NERC has demonstrated a lack of urgency in protecting the bulk power system. This was clearly evidenced on February 14, 2019 in the Senate Committee on Energy and Natural Resources hearing entitled: “Hearing to Consider the Status and Outlook for Cybersecurity Efforts in the Energy Industry.”⁷

Senator Angus King questioned NERC CEO James B. Robb on the supply chain risk management issue:

Sen. King: “Okay let me ask another question. Do any of our utilities have Kaspersky, Huawei, or ZTE equipment in their system?”

Mr. Robb: “We issued a NERC alert...”

Sen. King: “I didn’t ask you if you issued an alert. I asking you do any of our utilities have ZTE, Huawei, or Kaspersky equipment or software in their system?”

Mr. Robb: “Not to my knowledge.”

⁴ Available at: <https://www.ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf> (Accessed May 10, 2020).

⁵ See: <https://www.govinfo.gov/content/pkg/FR-2018-10-26/pdf/2018-23201.pdf> (Accessed May 10, 2020).

⁶ See 171 FERC ¶ 61,052, issued April 17, 2020.

⁷ Available at: <https://www.energy.senate.gov/public/index.cfm/hearings-and-business-meetings?ID=FE0534E7-2FC7-4DB0-BEA6-2634D3821ADD#> (accessed October 19, 2019).

Sen. King: “Not to your knowledge. Have you surveyed any of the utilities to determine that?”

Mr. Robb: “Uhhh, I don’t believe we have.”

Sen. King: “I think that would be a good idea, don’t you?”

Mr. Robb: “I’ll take that on.”

In other words, two and a half years after FERC ordered the Cyber Security Supply Chain Risk Management standard, NERC hadn’t even checked to see if there is Russian or Chinese equipment or software installed on the electric grid.

Complaint 1. The mandatory standard CIP-013-1 (Cyber Security - Supply Chain Risk Management) does not comport with Presidential Executive Order 13920.

Against the protest of numerous commenters in the docket, CIP-013-1 fails to cover all systems in the bulk power system. Section 4.2.3.5 of the standard excludes:

“Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP002-5, or any subsequent version of that Reliability Standard.”

In other words, the standard only covers high and medium impact systems and excludes supposed “low impact systems.” Unfortunately, the discretion is left to the individual companies in the industry to decide what is “low impact.”

On May 4, 2020, the President of the United States declared a national emergency and issued Executive Order 13920: “Securing the United States Bulk-Power System.” This action by the President is a vote of no-confidence in the lackadaisical and inadequate actions of FERC and NERC. The Commission and the ERO have not done enough to protect the bulk power system from cyber threats. This indictment of the lack of action on the part of FERC and the ERO must be remedied.

The Executive order requires that the Secretary of Energy:

- (i) identify bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary that poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the bulk-power system in the United States, poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States, or otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons; and
- (ii) develop recommendations on ways to identify, isolate, monitor, or replace such items as soon as practicable, taking into consideration overall risk to the bulk-power system.

This order invalidates the present scheme in CIP-013-1 in which each individual company has the discretion to decide the systems to which it wishes the standard to apply. The president of the United States has ordered the entire bulk power system protected.

Complaint 2. The Federal Energy Regulatory Commission (FERC) has not ensured that mandatory CIP standards fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

On May 21, 2008 Representative James R. Langevin, chairman of the House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, in his opening statement to a hearing on cybersecurity⁸ noted:

As time passes, I grow particularly concerned by NERC, the self-regulating organization responsible for ensuring the reliability of the bulk power system. Not only do they propose cybersecurity standards that, according to the GAO and NIST, are inadequate for protecting critical national infrastructure, but throughout the committee's investigation they continued to provide misleading statements about their oversight of industry efforts to mitigate the Aurora vulnerability.

If NERC doesn't start getting serious about national security, it may be time to find a new electric reliability organization. NERC can begin demonstrating its commitment by incorporating more of the NIST security controls in the next iteration of its reliability standards.

Emphasis added. That hearing was in 2008. Eleven years later, FERC and NERC had still failed to ensure that the mandatory CIP standards addressed the NIST cybersecurity framework. In September of 2019, the Government Accountability Office (GAO) issued a report⁹ finding:

The Federal Energy Regulatory Commission (FERC)—the regulator for the interstate transmission of electricity—has approved mandatory grid cybersecurity standards. However, it has not ensured that those standards fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Emphasis added. GAO include this table with their assessment of how well the current CIP standards address the NIST framework:

⁸ "Implications of Cyber Vulnerabilities on the Resilience and Security of the Electric Grid." Before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. (110th Congress) May 21, 2008. <https://www.gpo.gov/fdsys/pkg/CHRG-110hrg43177/pdf/CHRG-110hrg43177.pdf> (accessed October 24, 2019). Hearing video available at: <https://www.c-span.org/video/?205553-1/security-electric-grid> (accessed October 24, 2019).

⁹ U.S. Government Accountability Office. "Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid." GAO-19-332: Published: Aug 26, 2019. Publicly Released: Sep 25, 2019. Copy attached hereto as Exhibit B. Also available at: <https://www.gao.gov/products/GAO-19-332> (accessed October 22, 2019).

Extent to Which FERC-Approved Cybersecurity Standards Address the National Institute of Standards and Technology Cybersecurity Framework's Identify and Protect Functions			
Function	GAO assessment	Category	GAO assessment
Identify	●	Asset management	●
		Business environment	○
		Governance	●
		Risk assessment	●
		Risk management strategy	○
		Supply chain risk management	●
Protect	●	Identity management, authentication, and access control	●
		Awareness and training	●
		Data security	●
		Information protection processes and procedures	●
		Maintenance	●
		Protective technology	●

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

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

The President of the United States and Congress are not alone in their criticism of the lack of action by FERC and NERC to protect the bulk power system.

On September 6, 2019, Cybersecurity expert George Cotter submitted an assessment in FERC Docket AD19-18-000 and NP19-4-000 entitled “Security in the North American Grid, The Existential Threat. A White Paper.”¹⁰ Mr. Cotter pointed out that:

“only 1374 of a total of 16,412 BES Transmission Substations qualified for CIP Standards based on Kv power minimums (over 90% excluded) and of the qualifiers, only 550 (40%) were estimated by their utilities to be critical to BES Reliability.”

In other words, the vast majority of facilities in the bulk power system are excluded from the CIP standards by their very design.

On May 4, 2020, Cybersecurity expert Joe Weiss pointed out in his blog¹¹ that:

“China and Russia have directly attacked the control system vendor supply chains since at least 2010. Many of the systems exploited and affected by adversaries are still used in the U.S. bulk and distribution power systems. Moreover, vendors supplying bulk (and distribution) electric equipment for the U.S. electric system also supplied similar (often the same) bulk and distribution electric equipment to other countries, including China, Iran, Russia, and Pakistan. (I include distribution systems, as it often uses the same equipment as transmission systems, and transmission directly “talks” to distribution – more discussions on distribution follows). Even

¹⁰ Attached hereto as Exhibit C

¹¹ Attached hereto as Exhibit D

bulk power equipment manufactured in the U.S. often use servers, processors, software, etc. that come from China which makes assuring supply chain integrity so difficult.”

And the supply chain threat is not hypothetical – it has actually happened. In his most recent article,¹² Mr. Weiss points out:

“So why the EO now? Government and public utility procurement rules often push organizations into buying equipment due to price and without regard to origin or risk. In this case, it resulted in a utility having to procure a very large bulk transmission transformer from China. When the Chinese transformer was delivered to a US utility, the site acceptance testing identified electronics that should NOT have been part of the transformer – hardware backdoors. That transformer now resides at a government installation.”

Our electric grid supply chain has already been targeted by state actors, as reported by Mr. Weiss and also by the Wall Street Journal. In a January 10, 2019 article,¹³ the WSJ reported:

“A reconstruction of the hack reveals a glaring vulnerability at the heart of the country’s electric system. Rather than strike the utilities head on, the hackers went after the system’s unprotected underbelly—hundreds of contractors and subcontractors like All-Ways who had no reason to be on high alert against foreign agents. From these tiny footholds, the hackers worked their way up the supply chain. Some experts believe two dozen or more utilities ultimately were breached.”

On May 4, 2020, the President of the United States declared a national emergency and issued Executive Order 13920: “Securing the United States Bulk-Power System.” This is a true emergency and the Commission should act on this complaint with a sense of urgency.

Conclusion and Recommendations

The mandatory Critical Infrastructure Protection (CIP) standard CIP-013-1 (Cyber Security - Supply Chain Risk Management) does not comport with Presidential Executive Order 13920: Securing the United States Bulk-Power System.

As noted by Congress in 2008 and the GAO in 2019, the Federal Energy Regulatory Commission (FERC) has not ensured that mandatory CIP standards “fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework.”

1. The Commission should direct NERC to Modify CIP-013-1 (Cyber Security - Supply Chain Risk Management) to cover every piece of equipment in the bulk power system with no exceptions including purported “low impact” BES cyber systems. Utilities should not have the discretion to decide what parts of the bulk power system they wish to protect.

¹² Attached hereto as Exhibit E.

¹³ Smith, Rebecca. The Wall Street Journal. “America’s Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It.” January 10, 2019. <https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112> (accessed May 11, 2020).

2. The Commission should direct NERC to revamp all CIP standards to “fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework.”

Respectfully submitted,

A handwritten signature in blue ink, appearing to read 'MM', is positioned above the name Michael Mabee.

Michael Mabee

Attachment: 18 CFR § 385.206 Compliance Information

18 CFR § 385.206 Compliance Information

I Michael Mabee, hereby state the following:

18 CFR § 385.206(b) Contents. A complaint must:

(1) Clearly identify the action or inaction which is alleged to violate applicable statutory standards or regulatory requirements;

- Contained in Complaint

(2) Explain how the action or inaction violates applicable statutory standards or regulatory requirements;

- Contained in Complaint

(3) Set forth the business, commercial, economic or other issues presented by the action or inaction as such relate to or affect the complainant;

- A widespread power outage as a result of the lack of physical security could cause the loss of life and substantial damage to the local or national economy.

(4) Make a good faith effort to quantify the financial impact or burden (if any) created for the complainant as a result of the action or inaction;

- A widespread power outage as a result of the lack of physical security could cause the loss of life and substantial damage to the local or national economy.

(5) Indicate the practical, operational, or other nonfinancial impacts imposed as a result of the action or inaction, including, where applicable, the environmental, safety or reliability impacts of the action or inaction;

- A widespread power outage as a result of the lack of physical security could cause the loss of life and substantial damage to the local or national economy.

(6) State whether the issues presented are pending in an existing Commission proceeding or a proceeding in any other forum in which the complainant is a party, and if so, provide an explanation why timely resolution cannot be achieved in that forum;

- I am unaware of any open FERC docket which addresses Executive Order 13920 or GAO Report number GAO-19-332.

(7) State the specific relief or remedy requested, including any request for stay or extension of time, and the basis for that relief;

- Contained in "Conclusion and Recommendations" section of Complaint.

(8) Include all documents that support the facts in the complaint in possession of, or otherwise attainable by, the complainant, including, but not limited to, contracts and affidavits;

- Attached as exhibits to the Complaint

(9) State

(i) Whether the Enforcement Hotline, Dispute Resolution Service, tariff-based dispute resolution mechanisms, or other informal dispute resolution procedures were used, or why these procedures were not used;

- N/A
- (ii) Whether the complainant believes that alternative dispute resolution (ADR) under the Commission's supervision could successfully resolve the complaint;
 - N/A
- (iii) What types of ADR procedures could be used; and
 - N/A
- (iv) Any process that has been agreed on for resolving the complaint.
 - N/A

(10) Include a form of notice of the complaint suitable for publication in the Federal Register in accordance with the specifications in § 385.203(d) of this part. The form of notice shall be on electronic media as specified by the Secretary.

- Draft Notice Attached

(11) Explain with respect to requests for Fast Track processing pursuant to section 385.206(h), why the standard processes will not be adequate for expeditiously resolving the complaint.

- N/A

18 CFR § 385.206(c) Service. Any person filing a complaint must serve a copy of the complaint on the respondent, affected regulatory agencies, and others the complainant reasonably knows may be expected to be affected by the complaint. Service must be simultaneous with filing at the Commission for respondents. Simultaneous or overnight service is permissible for other affected entities. Simultaneous service can be accomplished by electronic mail in accordance with § 385.2010(f)(3), facsimile, express delivery, or messenger.

- A copy of this Complaint will be sent electronically to the Electric Reliability Organization ("ERO") simultaneously with my filing with the Commission.

Respectfully submitted,



Michael Mabee

Draft Notice

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Complaint of Michael Mabee
Related to Critical Infrastructure
Protection Reliability Standards

Docket No.

NOTICE OF COMPLAINT

()

Take notice that on [date filed], pursuant to section 215(d) of the Federal Power Act, 16 U.S.C. 824o(d) and Rule 206 of the Federal Energy Regulatory Commission's (Commission) Rules of Practice and Procedure, 18 CFR 385.206 (2019), Michael Mabee filed a formal complaint Michael Mabee, (Complainant) filed a formal complaint alleging that 1) The mandatory Critical Infrastructure Protection (CIP) standard CIP-013-1 (Cyber Security Supply Chain Risk Management) does not comport with Presidential Executive Order 13920: Securing the United States Bulk-Power System and, 2) The Federal Energy Regulatory Commission (FERC) has not ensured that mandatory CIP standards "fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework."

Complainant certifies that copies of the complaint were served on the contacts as listed on the Commission's list of Corporate Officials.

Any person desiring to intervene or to protest this filing must file in accordance with Rules 211 and 214 of the Commission's Rules of Practice and Procedure (18 CFR 385.211 and 385.214). Protests will be considered by the Commission in determining the appropriate action to be taken, but will not serve to make protestants parties to the proceeding. Any person wishing to become a party must file a notice of intervention or motion to intervene, as appropriate. The Respondent's answer and all interventions, or protests must be filed on or before the comment date. The Respondent's answer, motions to intervene, and protests must be served on the Complainants.

The Commission encourages electronic submission of protests and interventions in lieu of paper using the "eFiling" link at <http://www.ferc.gov>. Persons unable to file

electronically should submit an original and 5 copies of the protest or intervention to the Federal Energy Regulatory Commission, 888 First Street, NE, Washington, DC 20426.

This filing is accessible on-line at <http://www.ferc.gov>, using the “eLibrary” link and is available for review in the Commission’s Public Reference Room in Washington, DC. There is an “eSubscription” link on the web site that enables subscribers to receive email notification when a document is added to a subscribed docket(s). For assistance with any FERC Online service, please email FERCOnlineSupport@ferc.gov, or call (866) 208-3676 (toll free). For TTY, call (202) 502-8659.

Comment Date: 5:00 pm Eastern Time on (insert date).

Kimberly D. Bose,
Secretary.

Exhibit A
To May 11, 2020 Complaint
Submitted by Michael Mabee

Presidential Documents

Title 3—

Executive Order 13920 of May 1, 2020

The President

Securing the United States Bulk-Power System

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), and section 301 of title 3, United States Code,

I, DONALD J. TRUMP, President of the United States of America, find that foreign adversaries are increasingly creating and exploiting vulnerabilities in the United States bulk-power system, which provides the electricity that supports our national defense, vital emergency services, critical infrastructure, economy, and way of life. The bulk-power system is a target of those seeking to commit malicious acts against the United States and its people, including malicious cyber activities, because a successful attack on our bulk-power system would present significant risks to our economy, human health and safety, and would render the United States less capable of acting in defense of itself and its allies. I further find that the unrestricted acquisition or use in the United States of bulk-power system electric equipment designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in bulk-power system electric equipment, with potentially catastrophic effects. I therefore determine that the unrestricted foreign supply of bulk-power system electric equipment constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, which has its source in whole or in substantial part outside the United States. This threat exists both in the case of individual acquisitions and when acquisitions are considered as a class. Although maintaining an open investment climate in bulk-power system electric equipment, and in the United States economy more generally, is important for the overall growth and prosperity of the United States, such openness must be balanced with the need to protect our Nation against a critical national security threat. To address this threat, additional steps are required to protect the security, integrity, and reliability of bulk-power system electric equipment used in the United States. In light of these findings, I hereby declare a national emergency with respect to the threat to the United States bulk-power system.

Accordingly, I hereby order:

Section 1. Prohibitions and Implementation. (a) The following actions are prohibited: any acquisition, importation, transfer, or installation of any bulk-power system electric equipment (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States, where the transaction involves any property in which any foreign country or a national thereof has any interest (including through an interest in a contract for the provision of the equipment), where the transaction was initiated after the date of this order, and where the Secretary of Energy (Secretary), in coordination with the Director of the Office of Management and Budget and in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and, as appropriate, the heads of other executive departments and agencies (agencies), has determined that:

(i) the transaction involves bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and

(ii) the transaction:

(A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the bulk-power system in the United States;

(B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States; or

(C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

(b) The Secretary, in consultation with the heads of other agencies as appropriate, may at the Secretary's discretion design or negotiate measures to mitigate concerns identified under section 1(a) of this order. Such measures may serve as a precondition to the approval by the Secretary of a transaction or of a class of transactions that would otherwise be prohibited pursuant to this order.

(c) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the date of this order.

(d) The Secretary, in consultation with the heads of other agencies as appropriate, may establish and publish criteria for recognizing particular equipment and particular vendors in the bulk-power system electric equipment market as pre-qualified for future transactions; and may apply these criteria to establish and publish a list of pre-qualified equipment and vendors. Nothing in this provision limits the Secretary's authority under this section to prohibit or otherwise regulate any transaction involving pre-qualified equipment or vendors.

Sec. 2. Authorities. (a) The Secretary is hereby authorized to take such actions, including directing the timing and manner of the cessation of pending and future transactions prohibited pursuant to section 1 of this order, adopting appropriate rules and regulations, and employing all other powers granted to the President by IEEPA as may be necessary to implement this order. The heads of all agencies, including the Board of Directors of the Tennessee Valley Authority, shall take all appropriate measures within their authority as appropriate and consistent with applicable law, to implement this order.

(b) Rules and regulations issued pursuant to this order may, among other things, determine that particular countries or persons are foreign adversaries exclusively for the purposes of this order; identify persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries exclusively for the purposes of this order; identify particular equipment or countries with respect to which transactions involving bulk-power system electric equipment warrant particular scrutiny under the provisions of this order; establish procedures to license transactions otherwise prohibited pursuant to this order; and identify a mechanism and relevant factors for the negotiation of agreements to mitigate concerns raised in connection with subsection 1(a) of this order. Within 150 days of the date of this order, the Secretary, in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and, as appropriate, the heads of other agencies, shall publish rules or regulations implementing the authorities delegated to the Secretary by this order.

(c) The Secretary may, consistent with applicable law, redelegate any of the authorities conferred on the Secretary pursuant to this section within the Department of Energy.

(d) As soon as practicable, the Secretary, in consultation with the Secretary of Defense, the Secretary of the Interior, the Secretary of Homeland Security,

the Director of National Intelligence, the Board of Directors of the Tennessee Valley Authority, and the heads of such other agencies as the Secretary considers appropriate, shall:

(i) identify bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary that poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the bulk-power system in the United States, poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States, or otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons; and

(ii) develop recommendations on ways to identify, isolate, monitor, or replace such items as soon as practicable, taking into consideration overall risk to the bulk-power system.

Sec. 3. Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security. (a) There is hereby established a Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security (Task Force), which shall work to protect the Nation from national security threats through the coordination of Federal Government procurement of energy infrastructure and the sharing of risk information and risk management practices to inform such procurement. The Task Force shall be chaired by the Secretary or the Secretary's designee.

(b) In addition to the Chair of the Task Force (Chair), the Task Force membership shall include the following heads of agencies, or their designees:

(i) the Secretary of Defense;

(ii) the Secretary of the Interior;

(iii) the Secretary of Commerce;

(iv) the Secretary of Homeland Security;

(v) the Director of National Intelligence;

(vi) the Director of the Office of Management and Budget; and

(vii) the head of any other agency that the Chair may designate in consultation with the Secretary of Defense and the Secretary of the Interior.

(c) The Task Force shall:

(i) develop a recommended consistent set of energy infrastructure procurement policies and procedures for agencies, to the extent consistent with law, to ensure that national security considerations are fully integrated across the Federal Government, and submit such recommendations to the Federal Acquisition Regulatory Council (FAR Council);

(ii) evaluate the methods and criteria used to incorporate national security considerations into energy security and cybersecurity policymaking;

(iii) consult with the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council in developing the recommendations and evaluation described in subsections (c)(i) through (ii) of this section; and

(iv) conduct any other studies, develop any other recommendations, and submit any such studies and recommendations to the President, as appropriate and as directed by the Secretary.

(d) The Department of Energy shall provide administrative support and funding for the Task Force, to the extent consistent with applicable law.

(e) The Task Force shall meet as required by the Chair and, unless extended by the Chair, shall terminate once it has accomplished the objectives set forth in subsection (c) of this section, as determined by the Chair, and completed the reports described in subsection (f) of this section.

(f) The Task Force shall submit to the President, through the Chair and the Director of the Office of Management and Budget:

(i) a report within 1 year from the date of this order;

(ii) a subsequent report at least once annually thereafter while the Task Force remains in existence; and

(iii) such other reports as appropriate and as directed by the Chair.

(g) In the reports submitted under subsection (f) of this section, the Task Force shall summarize its progress, findings, and recommendations described in subsection (c) of this section.

(h) Because attacks on the bulk-power system can originate through the distribution system, the Task Force shall engage with distribution system industry groups, to the extent consistent with law and national security. Within 180 days of receiving the recommendations pursuant to subsection (c)(i) of this section, the FAR Council shall consider proposing for notice and public comment an amendment to the applicable provisions in the Federal Acquisition Regulation to implement the recommendations provided pursuant to subsection (c)(i) of this section.

Sec. 4. Definitions. For purposes of this order, the following definitions shall apply:

(a) The term “bulk-power system” means (i) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (ii) electric energy from generation facilities needed to maintain transmission reliability. For the purpose of this order, this definition includes transmission lines rated at 69,000 volts (69 kV) or more, but does not include facilities used in the local distribution of electric energy.

(b) The term “bulk-power system electric equipment” means items used in bulk-power system substations, control rooms, or power generating stations, including reactors, capacitors, substation transformers, current coupling capacitors, large generators, backup generators, substation voltage regulators, shunt capacitor equipment, automatic circuit reclosers, instrument transformers, coupling capacity voltage transformers, protective relaying, metering equipment, high voltage circuit breakers, generation turbines, industrial control systems, distributed control systems, and safety instrumented systems. Items not included in the preceding list and that have broader application of use beyond the bulk-power system are outside the scope of this order.

(c) The term “entity” means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

(d) The term “foreign adversary” means any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or its allies or the security and safety of United States persons.

(e) The term “person” means an individual or entity.

(f) The term “procurement” means the acquiring by contract with appropriated funds of supplies or services, including installation services, by and for the use of the Federal Government, through purchase, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated.

(g) The term “United States person” means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.

Sec. 5. Recurring and Final Reports to the Congress. The Secretary is hereby authorized to submit recurring and final reports to the Congress regarding the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

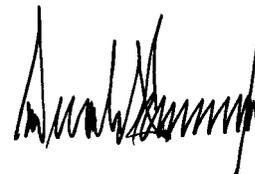
Sec. 6. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

A handwritten signature in black ink, appearing to be "Donald Trump", located on the right side of the page.

THE WHITE HOUSE,
May 1, 2020.

Exhibit B
To May 11, 2020 Complaint
Submitted by Michael Mabee



August 2019

CRITICAL INFRASTRUCTURE PROTECTION

Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid

GAO Highlights

Highlights of [GAO-19-332](#), a report to congressional requesters

Why GAO Did This Study

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

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

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

What GAO Recommends

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

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

August 2019

CRITICAL INFRASTRUCTURE PROTECTION

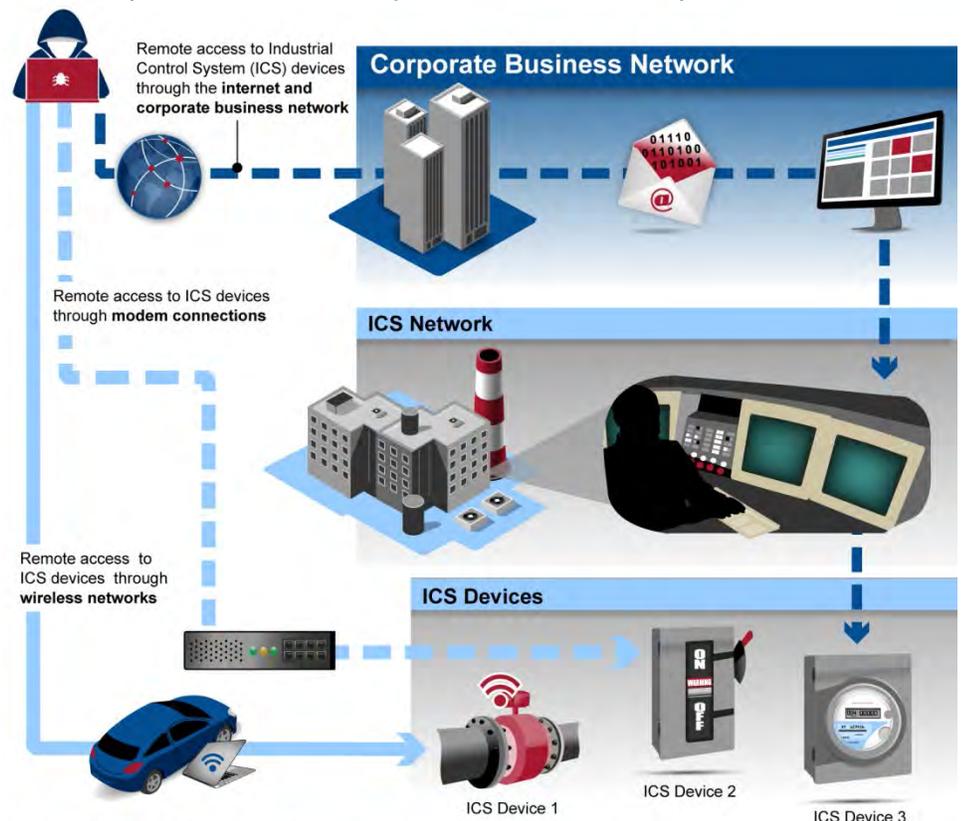
Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid

What GAO Found

The electric grid faces significant cybersecurity risks:

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

Potential Ways an Attacker Could Compromise Industrial Control System Devices



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

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

GAO is also making the following two recommendations to FERC:

1. Consider adopting changes to its approved cybersecurity standards to more fully address the NIST Cybersecurity Framework.
2. Evaluate the potential risk of a coordinated cyberattack on geographically distributed targets and, based on the results of that evaluation, determine if changes are needed in the threshold for mandatory compliance with requirements in the full set of cybersecurity standards.

DOE and FERC agreed with GAO's recommendations.

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

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

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

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

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

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

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

Contents

Letter		1
	Background	5
	The Grid Faces Significant Cybersecurity Risks and Challenges	16
	Federal Agencies Have Performed a Variety of Activities Aimed at Addressing Grid Cybersecurity Risks	35
	DOE Has Not Fully Defined a Strategy to Address Grid Cybersecurity Risks and Challenges	40
	FERC-Approved Standards Do Not Fully Address Grid Cybersecurity Risks	45
	Conclusions	52
	Recommendations for Executive Action	53
	Agency Comments, Third-Party Views, and Our Evaluation	53
Appendix I	Objectives, Scope, and Methodology	57
Appendix II	Assessment of the Extent FERC-Approved Cybersecurity Standards Address the NIST Cybersecurity Framework	63
Appendix III	Comments from the Department of Energy	70
Appendix IV	Comments from the Federal Energy Regulatory Commission	72
Appendix V	Comments from the North American Electric Reliability Corporation	74
Appendix VI	GAO Contacts and Staff Acknowledgments	77
Tables		
	Table 1: Federal Assessments of Cyberattacks and Electric Grid Operation Impacts of National Significance	29
	Table 2: DOE Plans and Assessment Addressing Electric Grid Cybersecurity Risks and Challenges	41

Table 3: Extent to Which DOE Grid Cybersecurity Plans and Assessment Address the Key Characteristics of a National Strategy	41
Table 4: National Institute of Standards and Technology (NIST) Cybersecurity Framework Functions and Categories	46
Table 5: Extent to Which Federal Energy Regulatory Commission-Approved Cybersecurity Standards Address NIST Cybersecurity Framework Functions and Categories	47
Table 6: Extent to Which Federal Energy Regulatory Commission-Approved Cybersecurity Standards for Medium- and High-Impact Systems Address NIST Cybersecurity Framework Categories and Subcategories	63

Figures

Figure 1: Functions of the Electric Grid	6
Figure 2: Three Interconnected Electric Transmission Grids Cover the Contiguous United States	7
Figure 3: Potential Ways an Attacker Could Compromise Industrial Control System Devices	24
Figure 4: Department of Homeland Security Vulnerability Advisories for Industrial Control System Devices, 2010 through 2018	26

Abbreviations

CIP	Critical Infrastructure Protection
DHS	Department of Homeland Security
DOE	Department of Energy
EIA	U.S. Energy Information Administration
FERC	Federal Energy Regulatory Commission
GPS	Global Positioning System
IoT	Internet of Things
IT	information technology
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
USB	universal serial bus

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



August 26, 2019

Congressional Requesters

The nation’s electric grid delivers the electricity that is essential for modern life. As a result, the reliability of the grid—its ability to meet consumers’ electricity demand at all times—has been of long-standing national interest. The grid’s reliability can be impaired by cyberattacks on the information technology (IT) systems that support its operations. Cybersecurity and industry experts have expressed concern that cyberattacks could result in widespread loss of electrical services—including long-duration, large-scale blackouts.

The federal government has a significant role in addressing cybersecurity risks facing the grid, even though most of the grid is owned and operated by private industry. 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.¹ The Department of Energy (DOE) was designated as the lead agency for federal efforts in the energy sector, which includes the grid. In addition, the Energy Policy Act of 2005 designated the Federal Energy Regulatory Commission (FERC) as the regulator for the interstate transmission of electricity with responsibility for reviewing and approving standards to provide for the reliable operation of the bulk power system.²

The security of federal cyber assets 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 2003.³ In September 2018, we issued

¹White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience* (Washington, D.C.: February 12, 2013).

²The term “bulk power system” refers to (1) facilities and control systems necessary for operating the interconnected electric transmission network and (2) the output from certain generation facilities needed for reliability. FERC oversees the North American Electric Reliability Corporation (NERC), 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.

³GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, [GAO-17-317](#) (Washington, D.C.: Feb. 16, 2017).

an update to this high-risk area that identified actions needed to address cybersecurity challenges facing the nation—including the development of a more comprehensive national strategy and better oversight.⁴ We also have identified *ensuring the cybersecurity of the nation* as one of nine high-risk areas that need especially focused executive and congressional attention.⁵

You asked us to review the cybersecurity of the electric grid. Our specific objectives were to (1) describe the cybersecurity risks and challenges facing the grid, (2) describe federal efforts to address grid cybersecurity risks, (3) assess the extent to which DOE has defined a strategy for addressing grid cybersecurity risks and challenges, and (4) assess the extent to which FERC-approved cybersecurity standards address grid cybersecurity risks.

To describe the cybersecurity risks and challenges facing the grid, we developed a list of cyber actors that could pose a threat to the grid, identified vulnerable components and processes that could be exploited, reviewed the potential impact of cyberattacks on the grid, and identified key cybersecurity challenges facing the grid. To develop the list of cyber threat actors, we reviewed our prior work on cyber-based threats facing the grid⁶ as well as the threats identified by the 2019 *Worldwide Threat Assessment of the U.S. Intelligence Community*.⁷ We also interviewed officials and representatives from key federal and nonfederal entities—20 federal entities (e.g., DOE and its national laboratories, the Department of Homeland Security [DHS], FERC), nine nonfederal entities (e.g., the

⁴GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, [GAO-18-622](#) (Washington, D.C.: Sept. 6, 2018).

⁵GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, [GAO-19-157SP](#) (Washington, D.C.: Mar. 6, 2019).

⁶GAO, *Cybersecurity: Challenges in Securing the Electric Grid*, [GAO-12-926T](#) (Washington, D.C.: July 17, 2012).

⁷Daniel 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.

North American Electric Reliability Corporation [NERC]⁸), and five grid owners and operators—to confirm, add, or remove cyber threat actors identified in our prior work based on their potential impact on grid operations.

To identify vulnerable components and processes, we reviewed reports produced by key federal and nonfederal entities related to grid vulnerabilities and met with these entities to understand the scale and complexity of these vulnerable components and processes. With respect to the potential impact of cyberattacks, we interviewed key federal entities and reviewed agency reports on grid incidents.⁹ We also reviewed federal studies assessing the potential for widespread power outages resulting from cyberattacks, and we met with federal officials to discuss the methodologies used to perform these studies.

Finally, to identify key cybersecurity challenges, we reviewed our prior reports on such challenges facing the grid,¹⁰ as well as federal and industry reports recommended by entities with whom we met. We also asked key federal and nonfederal entities, including grid owners and operators, to identify key challenges facing grid entities in addressing cybersecurity risks.

To describe federal efforts to address grid cybersecurity risks, we reviewed federal strategies, plans, and reports and interviewed officials from federal and nonfederal entities to identify critical infrastructure protection and regulatory actions that federal agencies are taking to address grid cybersecurity.¹¹ We categorized the critical infrastructure protection activities using the functions and categories in the National

⁸We include the NERC as a nonfederal entity here because it is a nonprofit corporation with membership by United States and Canadian entities that include utilities and other electric industry entities; municipal, state, regional, and federal regulators; regional transmission organizations and independent system operations; and electricity customers. However, as explained below, NERC nevertheless exercises some regulatory authority under FERC oversight.

⁹An incident is a security breach of a computerized system and information.

¹⁰GAO, *Electricity: Federal Efforts to Enhance Grid Resilience*, [GAO-17-153](#) (Washington, D.C.: January 2017); *Cybersecurity: Challenges in Securing the Modernized Electricity Grid*, [GAO-12-507T](#) (Washington, D.C.: Feb. 28, 2012); and [GAO-12-926T](#).

¹¹We did not review federal actions to address the cybersecurity of nuclear power plants, which are subject to standards issued by the Nuclear Regulatory Commission and are generally exempt from FERC-approved cybersecurity standards.

Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (commonly referred to as the NIST Cybersecurity Framework).¹²

To assess the extent to which DOE has defined a strategy for addressing grid cybersecurity risks and challenges, we analyzed the agency's efforts to develop approaches for implementing the federal cybersecurity strategy for the energy sector as it relates to the grid. Specifically, we compared DOE's grid cybersecurity plans and assessments against leading practices we identified in prior work on key characteristics for a national strategy.¹³

To assess the extent to which FERC-approved cybersecurity standards address grid cybersecurity risks, we compared those standards with the NIST Cybersecurity Framework¹⁴ and reviewed the applicability of the standards for bulk power entities. We also interviewed FERC officials to obtain information about current and future cybersecurity standards and oversight processes. Additional details on our objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from January 2018 to August 2019 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.

¹²National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (Gaithersburg, MD: April 2018). This voluntary, risk-based cybersecurity framework comprises a set of industry standards and best practices to help organizations manage cybersecurity risks.

¹³GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

¹⁴National Institute of Standards and Technology, *Cybersecurity Framework*.

Background

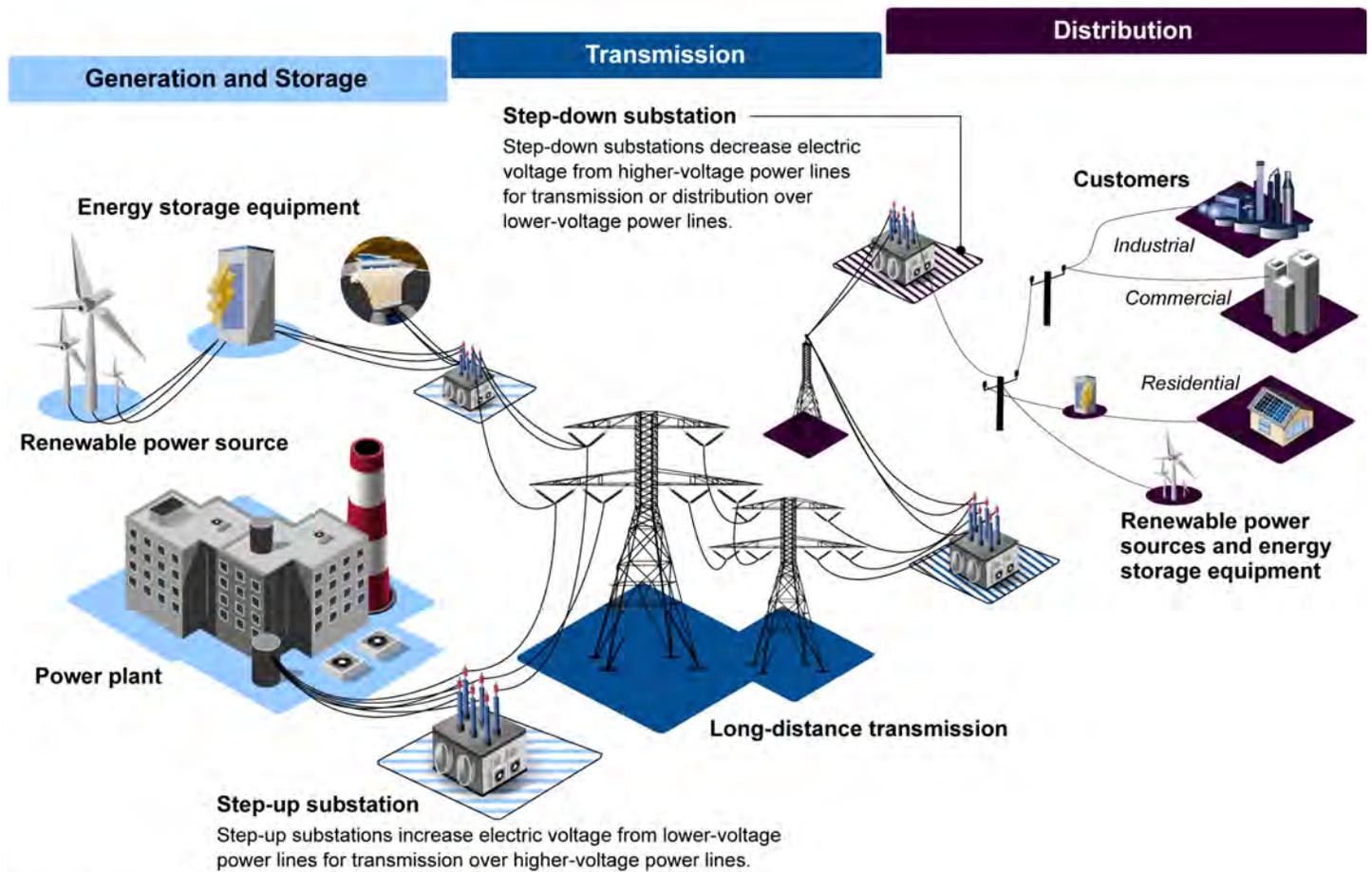
Grid Functions, Design, and Operations

The U.S. electric grid comprises three distinct functions: generation and storage, transmission, and distribution (see fig. 1).¹⁵

- **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 power transmission system connects geographically distant power plants with areas where electric power is consumed. Substations are used to transmit electricity at varied voltages and generally contain a variety of equipment, including transformers, switches, relays, circuit breakers, and system operations instruments and controls.
- **Distribution.** The distribution system carries electric power out of the transmission system to industrial, commercial, residential, and other consumers.

¹⁵The U.S. electric grid and its interconnections extend into Canada and Mexico.

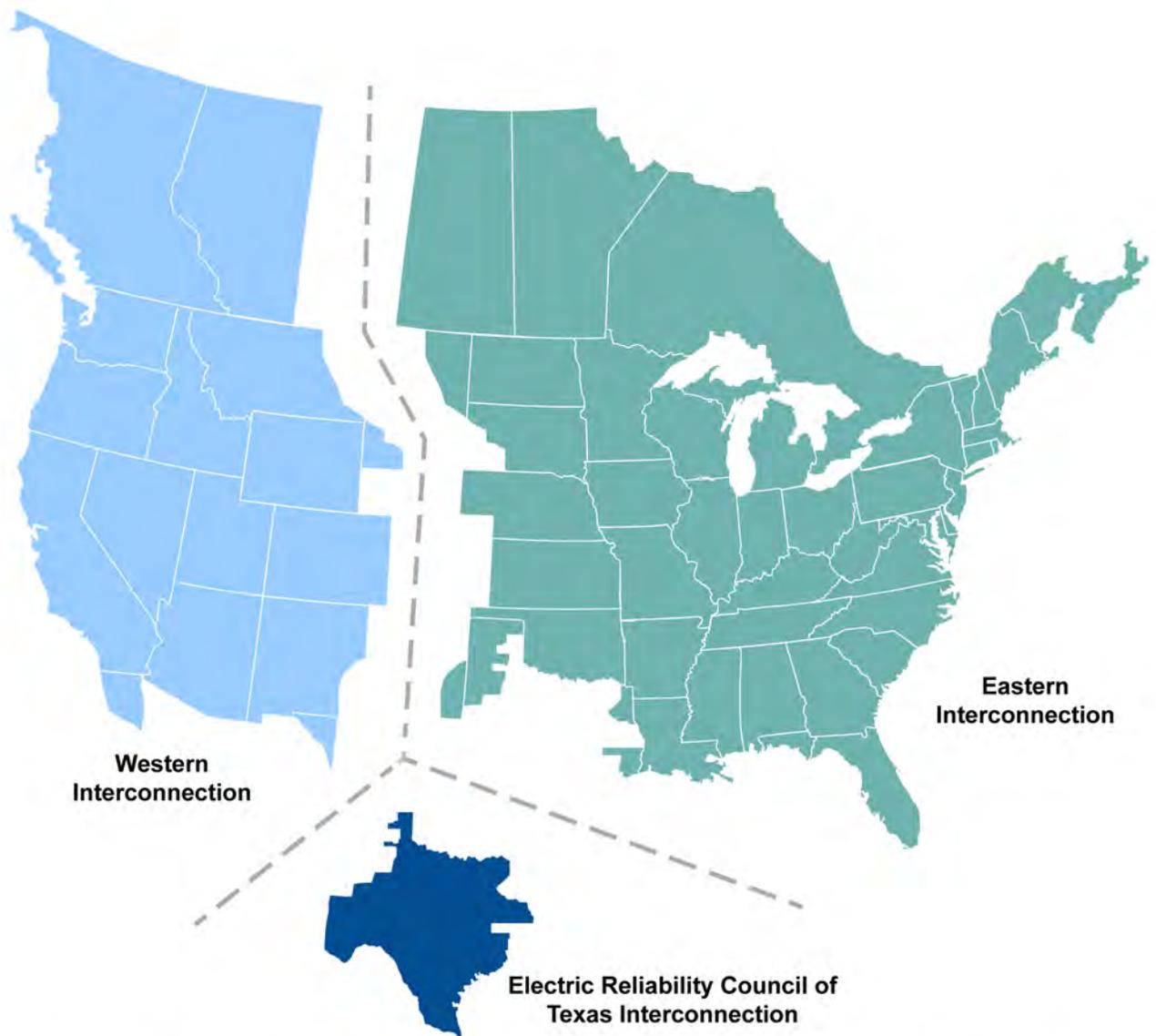
Figure 1: Functions of the Electric Grid



Sources: GAO; Art Explosion (images). | GAO-19-332

Three large electric grids, or interconnections, exist in the contiguous United States that collectively constitute the U.S. electric grid: the Eastern Interconnection, Western Interconnection, and Electric Reliability Council of Texas Interconnection (see fig. 2). These interconnections, which extend into parts of Canada and Mexico, operate independently with limited ability to move electric power between them; electric power is produced within an interconnection to meet demand in the same interconnection.

Figure 2: Three Interconnected Electric Transmission Grids Cover the Contiguous United States



Sources: This information from the North American Electric Reliability Corporation's website is the property of the North American Electric Reliability Corporation and is available at <https://www.nerc.com/AboutNERC/keyplayers/PublishingImages/Interconnections%2024JUL18.jpg>. This content may not be reproduced in whole or any part without the prior express written permission of the North American Electric Reliability Corporation. GAO (presentation). | GAO-19-332

The grid is generally considered to be resilient.¹⁶ Historically, grid operators have been able to respond quickly to the adverse consequences of an incident—whether it is damage from a major hurricane or a falling tree—and quickly restore service. In some cases, electricity may be restored long before utilities fully recover from an incident. For example, in instances with physical damage to grid components, such as an event that damages many substations, it could take months or years to fully restore the equipment.

The electricity industry has refined its power restoration processes after decades of experience in responding to disaster-related events, but restoration from a cyber-related event may be more challenging. For example, disaster-related events—such as hurricanes—may involve significant lead time before the incident. This allows owners and operators to take preemptive measures to protect their systems, develop restoration plans, and activate personnel. In contrast, cyberattacks may occur without warning, leaving owners and operators no time to prepare for a response. In addition, cyberattacks could target and damage specific types of components or facilities across a dispersed geographic area. Responding to such an attack could be more difficult than to a localized disaster-related event since resources may be geographically distributed rather than concentrated in the same area.

Industrial Control Systems Support the Grid

Industrial control systems are typically network-based systems that monitor and control sensitive processes and physical functions, such as the opening and closing of circuit breakers on the grid.¹⁷ These systems support the control of electric power generation, transmission, and distribution. System operators—which are sometimes affiliated with a particular utility or sometimes independent and responsible for multiple utility areas—manage electricity flows through these systems.

¹⁶According to DOE, resiliency refers to the ability of an energy facility to recover quickly from damage to any of its components or to any of the external systems on which it depends. Resiliency measures enable energy systems to continue operating despite damage and/or promote a rapid return to normal operations when damage and outages do occur. According to DOE officials, resiliency also includes measures to prevent damage from occurring.

¹⁷According to NIST, industrial control systems are used to control industrial processes such as manufacturing, product handling, production, and distribution. These systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

Early industrial control systems operated in isolation, running proprietary control protocols using specialized hardware and software. In addition, many industrial control system components were in physically secured areas, and the components were not connected to IT systems or the internet.

However, industrial control systems are changing in ways that offer advantages to system operators but that also make them more vulnerable to cyberattacks. In particular, proprietary devices in these systems are being replaced by cheaper and more widely available devices that use traditional IT networking protocols—including those that support remote access. These newer devices can provide the system operator with more detailed data on the conditions of the transmission and distribution systems and with better tools to observe and manage the grid. Remote access capabilities in the devices can also make them easier to maintain. Further, industrial control systems are being designed and implemented using traditional IT computers and operating systems, which allow corporate business and industrial control system networks to be connected more easily.

Nonetheless, cyberattacks on industrial control systems supporting grid operations may require a degree of sophistication and knowledge beyond what is needed to conduct cyberattacks on IT systems. For example, industrial control systems often use operating systems and applications that may be considered unconventional to typical IT personnel.

Critical Infrastructure Protection Roles, Responsibilities, and Key Initiatives

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

- **Presidential Policy Directive 21**, issued in February 2013, shifted the nation's focus from protecting critical infrastructure against terrorism to protecting and securing critical infrastructure and increasing its resilience against all hazards, including natural

disasters, terrorism, and cyber incidents.¹⁸ The directive identified 16 critical infrastructure sectors,¹⁹ such as the energy sector, which includes the grid. In addition, the directive identified energy and communications systems as uniquely critical because of the enabling functions they provide across all sectors.

The directive also outlined roles and responsibilities for protecting these sectors. For example:

- The directive designated DOE as the sector-specific agency for the energy sector. According to the directive, DOE and other sector-specific agencies are responsible for, among other things, collaborating with critical infrastructure owners and operators, identifying vulnerabilities, and helping to mitigate incidents. In addition, the Fixing America's Surface Transportation Act of 2015 codified DOE's role as the sector-specific agency for the energy sector and gave DOE 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.²⁰ The Office of Cybersecurity, Energy Security, and Emergency Response is the lead for DOE's energy sector cybersecurity efforts.
- The directive called for DHS to coordinate the overall federal effort to promote the security and resilience of the nation's critical infrastructure. Within DHS, the Cybersecurity and Infrastructure Security Agency's National Cybersecurity and Communications Integration Center is the lead for cyber and physical infrastructure

¹⁸White House, *Presidential Policy Directive 21/PPD-21: Critical Infrastructure Security and Resilience*. The directive defines the term "all hazards" as a threat or an incident, natural or manmade, which warrants action to protect life, property, the environment, and public health or safety and to minimize disruptions of government, social, or economic activities. "All hazards," as further defined in the directive, includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure. The directive defines "resilience" as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions and includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

¹⁹The 16 critical infrastructure sectors are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

²⁰Pub. L. No. 114-94, Div. F, § 61003(a).

security. Private-sector critical infrastructure owners and operators are encouraged, but not required, to report cybersecurity incidents to the center.²¹

- The directive emphasized that critical infrastructure owners and operators 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**, updated by DHS in December 2013, among other things, further integrates critical infrastructure protection efforts between government and private sectors.²² It describes a voluntary partnership model as the primary means of coordinating government and private-sector efforts to protect critical infrastructure. As part of the partnership structure, the designated sector-specific agencies serve as the lead coordinators for the security programs of their respective sectors.

The plan also called for each sector to have a government coordinating council,²³ consisting of representatives from various levels of government, and many sectors have a coordinating council consisting of owner-operators of these critical assets or members of their respective trade associations.²⁴ 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.

²¹As articulated in the National Cybersecurity Protection Act of 2014, the term “incident” means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

²²Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (December 2013).

²³Government coordinating councils coordinate strategies, activities, policy, and communications across government entities within each sector and consist of representatives across various levels of government (e.g., federal, state, local, and tribal), as appropriate. For example, DHS and DOE are designated as the co-chairs of the Energy Sector Government Coordinating Council.

²⁴Sector coordinating councils are self-organized, self-run, and self-governed private sector councils that interact on a wide range of sector-specific strategies, policies, and activities. Membership on the councils can vary from sector to sector but is meant to represent a broad base of owners, operators, associations, and other entities—both large and small—within the sector.

-
- **Executive Order 13636: Improving Critical Infrastructure Cybersecurity**, issued in 2013, among other things, addresses the need to improve cybersecurity through information sharing and collaboratively developing and implementing risk-based standards.²⁵ It called for NIST to lead the development of a framework to reduce cybersecurity risks to critical infrastructure. It also called for sector-specific agencies to develop mechanisms to encourage adoption of the framework. NIST issued its Cybersecurity Framework in 2014 and updated it in April 2018.²⁶ The framework provides a set of cybersecurity activities, desired outcomes, and applicable references that are common across all critical infrastructure sectors, including the energy sector.

The executive branch has taken steps toward outlining a federal strategy for confronting cyber threats—including those facing critical infrastructure such as the grid. For example:

- **Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure**, issued in May 2017, required federal agencies to take a variety of actions aimed at improving the cybersecurity of federal networks and critical infrastructure.²⁷ Among other things, the order required DOE and DHS to assess the potential scope and duration of a prolonged power outage associated with a significant cyber incident, 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.
- **The National Cyber Strategy**, issued in September 2018, builds upon Executive Order 13800 and describes actions that federal agencies and the administration are to take to, among other things, secure critical infrastructure. For example, one of the strategy's seven goals is protecting critical infrastructure. To achieve this goal, the strategy outlines a number of priority actions, such as prioritizing risk-reduction across seven key areas, including energy and power.
- **The DHS Cybersecurity Strategy** was released in May 2018 with the intent of providing the department with a framework to execute cybersecurity responsibilities during the next 5 years. The plan

²⁵Exec. Order No. 13636, 78 Fed. Reg. 11,737 (Feb. 19, 2013).

²⁶National Institute of Standards and Technology, *Cybersecurity Framework*.

²⁷Exec. Order No. 13800, 82 Fed. Reg. 22,391 (May 16, 2017).

outlines seven goals the department plans to accomplish in support of its mission related to managing national cybersecurity risks. For example, for the goal of protecting critical infrastructure, the plan outlines a number of objectives and sub-objectives, such as expanding and improving the sharing of cyber threat indicators, defensive measures, and other cybersecurity information.

In our 2018 and 2019 updates on government high-risk areas, we reported that these executive branch strategy documents did not include key elements of desirable characteristics that can enhance the usefulness of a national strategy as guidance for decision makers in allocating resources, defining policies, and helping to ensure accountability.²⁸

Electric Grid Cybersecurity Regulation

Federal and state authorities play key roles in regulating the reliability of the grid, which can be impaired by cybersecurity attacks. FERC is the federal regulator of interstate transmission of electricity with responsibility to review and approve standards to provide for the reliable operation of the bulk power system. In addition, FERC oversees NERC, which is the federally designated U.S. electric reliability organization.²⁹ NERC is responsible for conducting reliability assessments and enforcing mandatory standards to ensure the reliability of the bulk power system—a term that 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.³⁰ NERC develops reliability standards collaboratively through a deliberative process involving utilities

²⁸[GAO-18-622](#) and [GAO-19-157SP](#).

²⁹Under 16 U.S.C. § 824o, the U.S. electric reliability organization is the organization certified by FERC to establish and enforce reliability standards within the bulk-power system, subject to FERC review.

³⁰NERC also implements non-regulatory programs aimed at enhancing grid cybersecurity. For example, NERC leads GridEX, a large, geographically distributed grid security exercise conducted every other year involving industry and government that attempts to execute the electricity subsector's emergency response to simulated cyber and physical security threats and incidents, strengthen utilities' crisis response functions, and provide input for lessons learned. In addition, NERC operates the Electricity Information Sharing and Analysis Center which, in collaboration with DOE and the Electricity Subsector Coordinating Council, gathers and analyzes security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the electricity subsector.

and others in the electricity industry.³¹ NERC then sends the standards to FERC, which can either approve them or remand them to NERC for revision.³²

These reliability standards include critical infrastructure protection standards for protecting electric utility-critical and cyber-critical assets from cyberattacks. FERC has approved 11 such cybersecurity standards, 10 of which are currently enforced.³³

The standards call for organizations to classify their cyber systems as low-, medium-, or high-impact based on the adverse impact that loss, compromise, or misuse of those systems could have on the reliable operation of the bulk electric system. The classifications are made based on criteria and associated thresholds for, among others, generation resources and transmission substation operations. In turn, the standards apply differently to cyber systems based on whether they are classified as low-, medium-, or high-impact systems. For example:

- **Low-impact systems.** Systems that affect net aggregate generation capacity of less than 1,500 megawatts at one power plant location within a single interconnection are classified as low-impact systems

³¹Prior to submission to FERC for approval, NERC standards are reviewed and voted on by members of the electricity industry who participate in NERC's FERC-approved standards development process.

³²These standards become mandatory and enforceable in the contiguous United States only after FERC approval.

³³The 10 currently enforced cybersecurity standards are CIP-002-5.1a: Bulk Electric System Cyber System Categorization, CIP-003-6: Security Management Controls, CIP-004-6: Personnel & Training, CIP-005-5: Electronic Security Perimeter(s), CIP-006-6: Physical Security of Bulk Electric System Cyber Systems, CIP-007-6: System Security Management, CIP-008-5: Incident Reporting and Response Planning, CIP-009-6: Recovery Plans for Bulk Electric System Cyber Systems, CIP-010-2: Configuration Change Management and Vulnerability Assessments, and CIP-011-2: Information Protection. The 11th cybersecurity standard—CIP-013-1: Supply Chain Risk Management—will be subject to enforcement by July 2020. In addition, updates to four of the standards will become enforceable over the next two years: CIP-003-7 (enforceable by January 2020), CIP-005-6 and CIP-010-3 (enforceable by July 2020), and CIP-008-6 (enforceable by January 2021).

and are subject to the requirements in two of the 11 cybersecurity standards.³⁴

- **Medium-impact systems.** Systems that similarly affect net aggregate generation capacity of at least 1,500 megawatts are classified as medium-impact systems and are subject to requirements in the full set of cybersecurity standards.
- **High-impact systems.** Systems that are used by and located at certain control centers are classified as high-impact systems and are subject to the full set of cybersecurity standards. The standards generally require organizations to implement similar controls for medium- and high-impact systems, with more stringent variations of certain controls for high-impact systems.

As of December 2017, at most about 20 percent of the nation's generation capacity comes from power plants with medium-impact systems and therefore is subject to requirements in the full set of cybersecurity standards.³⁵

Both NERC and FERC have authority to enforce reliability standards. In addition, FERC has the authority to oversee NERC's enforcement of the FERC-approved reliability standards.

Cyber incident reporting is also an important part of federal and nonfederal regulatory efforts. Federal law requires grid owners and operators to report bulk power system incidents to DOE when certain criteria are met, such as a cyber event that causes interruptions of

³⁴The requirements that apply to low-impact systems are within CIP-002-5.1a: Bulk Electric System Cyber System Categorization and CIP-003-6: Security Management Controls. While low-impact systems are not subject to the requirements of the other eight currently enforced cybersecurity standards, organizations with such systems are required to implement cybersecurity policies and plans that address some topics covered in those standards, including physical security controls, certain electronic controls, cybersecurity awareness, and cybersecurity incident response. According to NERC, the level of protection for low-impact systems reflects the level of risk that the misuse or unavailability of those systems would pose to the bulk electric system.

³⁵According to NERC officials, the percentage of the nation's generation capacity at power plants with medium-impact systems is less than 20 percent because NERC encourages entities to disaggregate their industrial control systems so that individual systems operate and maintain less than 1,500 megawatts of generation capacity. NERC officials stated that such low-impact systems do not store high-value information and, in many cases, do not possess remote or networked communications capability. As a result, NERC has determined that the misuse, degradation, or destruction of those systems would have a minimal impact on the reliability of the bulk electric system.

electrical system operations or that could potentially affect power system reliability.³⁶ In addition, FERC-approved reliability standards require certain registered grid owners and operators to report cybersecurity incidents—that is, cybersecurity events that have compromised or disrupted one or more reliability tasks—to NERC.³⁷

State regulators generally oversee the reliability of distribution systems, and cybersecurity regulations related to the distribution grid may vary across states. In 2017, the National Association of Regulatory Utility Commissioners released an updated version of its cybersecurity primer for state utility regulators that aims to provide guidance to state regulators. The primer highlights the NIST Cybersecurity Framework as well as the FERC-approved cybersecurity standards as helpful tools for utilities and state regulators.

The Grid Faces Significant Cybersecurity Risks and Challenges

The U.S. electric grid faces significant cybersecurity risks—that is, threats, vulnerabilities, and impacts—and grid owners and operators face significant challenges in addressing these risks. Threat actors are becoming increasingly capable of carrying out attacks on the grid. At the same time, the grid is becoming more vulnerable to attacks. With respect to the potential impacts of the threats and vulnerabilities, U.S. cybersecurity incidents reportedly have not caused a domestic power outage. In addition, federal agencies have performed three assessments of the potential impacts that cyberattacks could have on the grid, but the potential scale of any associated outages is uncertain due to limitations in the assessments. As grid owners and operators attempt to address cybersecurity risks, they face a number of challenges, such as difficulties in hiring a sufficient cybersecurity workforce and limited public-private information sharing.

Various Cyber Threat Actors Are Increasingly Capable of Attacking the Grid

A variety of threat actors pose significant cybersecurity threats to the electric grid, and many of these threat actors are becoming increasingly adept at carrying out attacks on industrial control systems, such as those supporting grid operations. Relatedly, the skill needed to attack industrial

³⁶Section 13(b) of the Federal Energy Administration Act of 1974 (Public Law 93-275).

³⁷In July 2018, FERC directed NERC to modify its cybersecurity standards to lower the threshold for reporting cybersecurity events to NERC.

control systems is decreasing, as tools for exploiting industrial control system vulnerabilities become more available.

According to the 2019 *Worldwide Threat Assessment of the U.S. Intelligence Community*, nations, criminal groups, and terrorists pose the most significant cyber threats to U.S. critical infrastructure.³⁸ In addition, hackers and hacktivists, as well as insiders, pose significant cyber threats to the grid, according to officials and representatives of key federal and nonfederal entities whom we interviewed.

Nations

Nations, including nation-state, state-sponsored, and state-sanctioned groups or programs, use cyber tools as part of their information-gathering and espionage activities. According to the 2019 *Worldwide Threat Assessment*, China and Russia pose the greatest cyberattack threats;³⁹ of particular concern, they possess the ability to launch cyberattacks that could cause localized, temporary disruptive effects on critical infrastructure. For example, the assessment states that China has the ability to disrupt a natural gas pipeline for days to weeks (which could in turn disrupt grid operations), and Russia has the ability to disrupt an electrical distribution network for at least a few hours. The assessment also states that Russia is mapping U.S. critical infrastructure with the long-term goal of being able to cause substantial damage. Separately, DHS and the Federal Bureau of Investigation have described Russian

³⁸The assessment also noted that the growing availability and use of publicly and commercially available cyber tools is increasing the overall volume of unattributed cyber activity around the world.

³⁹The 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.

activities as an intrusion campaign by actors on U.S. government entities and critical infrastructure organizations.⁴⁰

In addition, a nation-state has successfully demonstrated its capability to disrupt the grid of another country. Specifically, according to the Office of the Director of National Intelligence, in December 2015 a state-sponsored actor conducted a cyberattack on the Ukrainian power grid that systematically disconnected substations, resulting in a power outage that lasted 3 hours.⁴¹

Officials and representatives of key federal and nonfederal entities we interviewed identified nations as the most capable threat actor but also noted that nations may not take action to disrupt the U.S. grid. For example, representatives from two utilities stated that nation-state actors are of the most concern because they have the resources to persist in their operations. However, officials from Los Alamos National Laboratory explained that nation-states may choose not to sponsor an attack because they could be easily identified. In addition, a representative from one of the utilities that we met with stated that nation-states may not pursue a cyberattack on the U.S. grid because they may be concerned about the potential response by the United States. Federal officials we interviewed noted that nation-states may be interested in gathering information about U.S. critical infrastructure with the intent of conducting a cyberattack at a later date.

Criminal Groups

Criminal groups, including organized crime organizations, seek to use cyberattacks for monetary gain. According to the 2019 *Worldwide Threat Assessment*, financially motivated cyber criminals will likely expand their

⁴⁰Specifically, DHS's National Cybersecurity and Communications Integration Center and the Federal Bureau of Investigation characterized the intrusions as a Russian multi-stage intrusion campaign by actors on U.S. government entities and organizations within the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. According to the agencies, the campaign targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the actors conducted network reconnaissance, moved laterally, and collected information pertaining to industrial control systems. Federal Bureau of Investigation and National Cybersecurity and Communications Integration Center, *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, TA18-074A (Washington, D.C.: March 16, 2018 [revised]).

⁴¹Office of the Director of National Intelligence. NFCA/E-ISAC Rapid Deployment Project, accessed March 4, 2019, <https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-blog/2510-nfca-e-isac-rapid-deployment-project>.

targets in the United States in the next few years, and their actions could disrupt critical infrastructure in non-energy sectors.

The intelligence community does not identify criminal groups as a threat specifically to the energy sector, but these groups could still have a large impact on the grid. For example, criminal organizations often use ransomware—malicious software used to deny access to IT systems or data—to hold systems or data hostage until a ransom is paid. Criminal groups have not used ransomware to target industrial control systems, but ransomware has been used to infect IT systems tied to industrial control systems. For example, the Center for Internet Security reported in March 2019 that the LockerGoga ransomware disrupted industrial and manufacturing firms’ networks, including a Norwegian aluminum company, which had to temporarily move to manual production.⁴² According to DHS’s Industrial Control Systems Computer Emergency Response Team, ransomware continues to be a major threat to both IT and industrial control systems that support the grid.

In addition, officials and representatives of key federal and nonfederal entities we interviewed suggested that nations could hire criminal groups to achieve their objectives. For example, an official from the National Renewable Energy Laboratory stated that criminal groups could be leveraged by other threat actors that have different incentives, such as nations focused on intelligence-gathering operations.

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. Terrorist groups may be highly motivated to disrupt or damage the grid, but 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*. However, terrorist groups could cause disruptive effects, such as defacing websites or executing denial-of-service attacks⁴³ against poorly protected networks.

⁴²Center for Internet Security, *Security Primer – LockerGoga*, accessed May 2, 2019, <https://www.cisecurity.org/white-papers/security-primer-lockergoga/>.

⁴³According to NIST, a denial-of-service attack prevents authorized access to resources or delays time-critical operations.

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 to make a point. Hackers and hacktivists no longer need a great amount of skill to compromise IT systems because they can download commonly available attack tools.

Officials and representatives of key federal and nonfederal entities we interviewed told us that hackers and hacktivists may have less capability to do harm than the most significant threat actors identified by the intelligence community, but they still pose a threat to the grid. For example, officials from the National Energy Technology Laboratory explained that while hacktivists generally are less capable than nations, their intent to inflict harm or to damage operations is typically more immediate than nations' longer-term goals. In addition, representatives from nonfederal entities stated that hacktivists may be capable of causing problems for electric utilities and systems supporting the delivery of power.

Insiders

Insiders are entities (e.g., employees, contractors, vendors) with authorized access to an information system or enterprise who have the potential to cause harm through destruction, disclosure, modification of data, or denial of service. Such destruction can occur wittingly or unwittingly. For example, in 2009, a disgruntled former IT employee of a Texas power plant allegedly disrupted the company's energy forecast system when the company failed to deactivate the employee's account access and confiscate his company-issued laptop after firing him two days earlier.

By contrast, in another case in 2009, contractors were reported to have unwittingly introduced malware on a uranium enrichment facility's workstations in Iran. Specifically, the attackers introduced malware on the contractor's business network. The malware then reportedly spread to universal serial bus (USB) devices that were used to transfer information between the contractors' business IT network and the uranium enrichment facility's workstations.⁴⁴

⁴⁴Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York, N.Y.: Crown Publishing Group, 2014).

Officials and representatives of key federal and nonfederal entities that we interviewed stated that while the threat posed by insiders varies, they could cause damaging effects. For example, Sandia National Laboratories officials explained that insiders could include knowledgeable employees with privileged access to critical systems or contractors with limited system knowledge. Further, representatives from another nonfederal entity explained that insider threats are a concern because of the economically valuable information they could steal.

The Grid Is Becoming More Vulnerable to Cyberattacks

The electric grid is becoming more vulnerable to cyberattacks via (1) industrial control systems, (2) consumer Internet of Things (IoT)⁴⁵ devices connected to the grid's distribution network, and (3) the global positioning system (GPS).⁴⁶

Industrial Control Systems

As previously noted, cheaper and more widely available devices that use traditional IT networking protocols are being integrated into industrial control systems. The use of these protocols, as well as traditional IT computers and operating systems, has led to a larger cyberattack surface—the different points in a network where attackers can try to enter or extract information—for the grid's systems.

In particular, many industrial control system devices include remote access capabilities, and industrial control systems are increasingly connected to corporate business networks.

- **Remote access capabilities.** Vendors are increasingly including remote access capabilities, including modems and wireless networking, as part of industrial control system devices. These capabilities are susceptible to exploitation by malicious actors. For example, malicious actors could scan a range of potential telephone numbers common to an area or published on a company website to find open modem connections to these devices (referred to as “war dialing”). In addition, malicious actors could scan for unsecured

⁴⁵IoT is generally defined as the concept of connecting and interacting through a network with a broad array of “smart” devices, such as building energy management systems, thermostats, or electric vehicle charging stations.

⁴⁶GPS is a global positioning, navigation, and timing system consisting of space, ground control, and user equipment segments that support the broadcasts of military and civil GPS signals.

wireless networks connected to industrial control system devices while in close proximity to the devices (referred to as “war driving”).⁴⁷

If implemented effectively, modern cybersecurity practices often protect against techniques used to remotely access industrial control system devices, and only allow trusted connections. However, to circumvent these practices, a malicious actor could, for example, compromise a vendor’s network—which is often trusted by owners and operators—and use the trusted connection to remotely connect to industrial control system devices.⁴⁸

- **Connections to corporate business networks.** Industrial control systems, which were once largely isolated from the internet and business IT systems, are increasingly connected in modern energy systems, allowing cyberattacks to originate in business IT systems and migrate to industrial control systems. For example, malicious nation-state actors used spear phishing⁴⁹ emails to deploy malware on business IT networks in the 2015 attack on Ukrainian electricity utilities. After gaining initial access to the business IT networks, the attackers reportedly used a variety of techniques to migrate to the industrial control system networks of the utilities.

Moreover, even if industrial control systems are not physically connected to business IT systems, malicious actors can exploit the use of removable media between the two networks. For example, as previously mentioned, contractors were reported to have unwittingly introduced malware on uranium enrichment facility workstations in Iran by using USB devices that were infected with the malware on the

⁴⁷In addition to “war driving” and “war dialing,” websites with search engine capabilities may provide information regarding unsecured industrial control system devices. For example, the website Shodan gathers data on unsecured industrial control system devices such as location and system software.

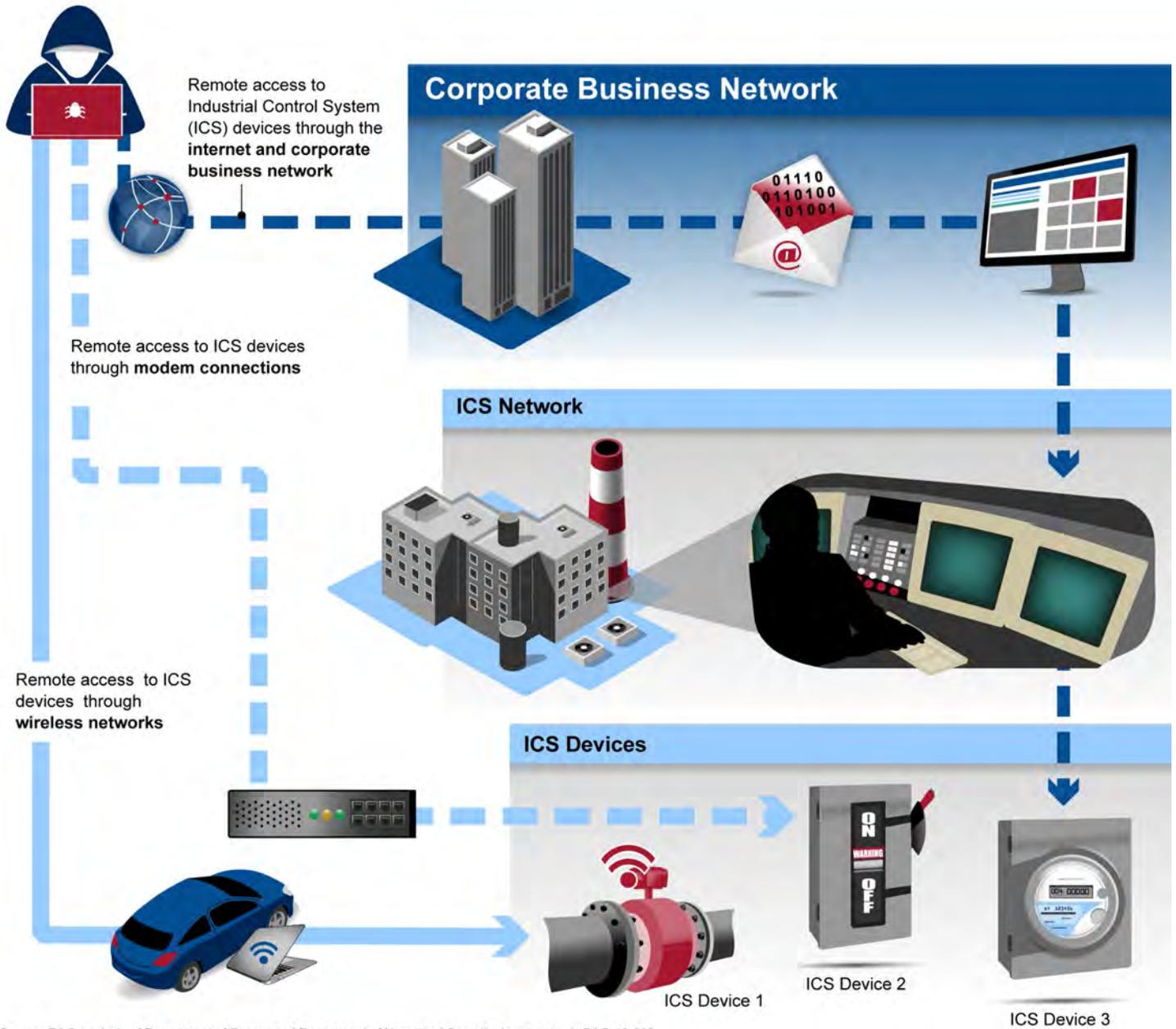
⁴⁸For example, according to a 2014 alert from DHS’s Industrial Control Systems Computer Emergency Response Team, attackers infected software installers on industrial control system vendor websites with a software Trojan known as Havex for the purpose of infecting devices across several critical infrastructures. According to the alert, these techniques could have allowed the attackers to access the networks of systems that installed the infected software. Department of Homeland Security, Industrial Control Systems Computer Emergency Response Team, *ICS Focused Malware (Update A)*, ICS-ALERT-14-178-01 (Washington, D.C.: Last revised August 22, 2018).

⁴⁹Spear phishing is a colloquial term that can be used to describe any highly targeted phishing attack. A phishing attack is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

contractors' business IT network to transfer information to the uranium enrichment facility's workstations.

Figure 3 illustrates how malicious actors could leverage this increasing attack surface to compromise industrial control systems.

Figure 3: Potential Ways an Attacker Could Compromise Industrial Control System Devices



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

Compounding the risk associated with the increased attack surface, many legacy industrial control systems were not designed with cybersecurity protections because they were not intended to be connected 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.

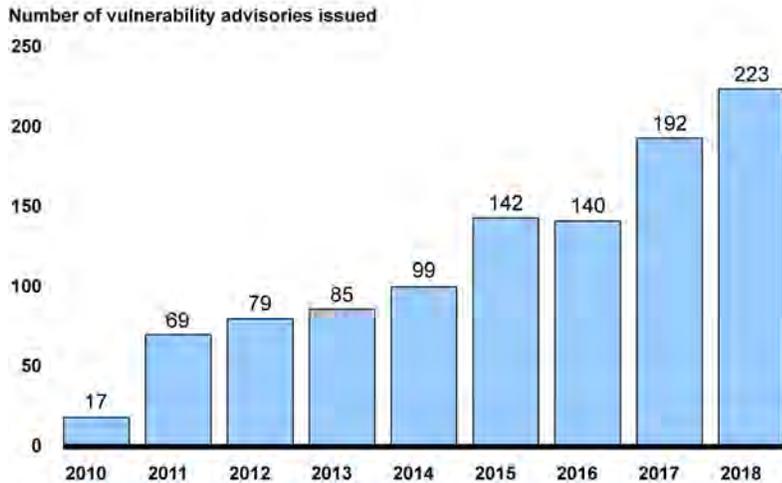
Additionally, even in the case of more modern devices, the safety and efficiency goals of the grid and the supporting industrial control systems can conflict with the goal of security in the design and operation of industrial control systems. According to an Idaho National Laboratory analysis, grid owners and operators may not always be able to identify industrial control system vulnerabilities in a timely manner.⁵⁰ Vulnerability scanning is often used in IT systems to validate proper system configuration and to identify any vulnerabilities that may be present. However, conventional IT vulnerability scanning can disable or shut down energy delivery systems, and testing may not always detect vulnerabilities deep within industrial control system software.

Further, even if owners and operators are able to identify industrial control system cybersecurity vulnerabilities, they may not be able to address those vulnerabilities in a timely manner because certain industrial control system devices may have high availability requirements to support grid operations. These devices typically need to be taken offline to apply patches to fix cybersecurity vulnerabilities. In addition, grid owners and operators need to rigorously test the patches before applying them. Security patches are typically tested by vendors, but they can degrade or alter the functionality of industrial control systems, which can have serious consequences for grid operations.

Consequently, there is increased risk that malicious actors may be able to exploit vulnerabilities in industrial control system devices before patches can be applied. According to DHS, the number of vulnerability advisories for industrial control systems devices has steadily increased, from 17 advisories in 2010 to 223 advisories in 2018 (see fig. 4).

⁵⁰Mission Support Center, Idaho National Laboratory, INL/EXT-16-40692, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector* (August 2016).

Figure 4: Department of Homeland Security Vulnerability Advisories for Industrial Control System Devices, 2010 through 2018



Source: GAO summary of Department of Homeland Security website information. | GAO-19-332

Moreover, supply chains for industrial control systems can introduce vulnerabilities that could be exploited for a cyberattack.⁵¹ For example, there is a potential for manufacturers and developers to—wittingly or unwittingly—include unauthorized code or malware in industrial control system devices and systems that provides a back door into the equipment or that allows the program to “call home” once installed. Further, manufacturers and software developers create their products in many different locations around the world, thus making them potentially susceptible to foreign-based threats. For example, a capable nation-state could gather useful information on the types of equipment used at a particular utility with the intent to undermine security controls at a later time.

In addition, manufacturers and developers have made sensitive information publicly available regarding the operation of their hardware and software. For example, manufacturers and developers have published vendor manuals, which include information such as default

⁵¹ Supply chains are a linked set of resources and processes between acquirers, integrators, and suppliers that begin with the design of products and services and extend through development, sourcing, manufacturing, handling, and delivery of products and services to the acquirer.

Consumer IoT Devices Connected to the Grid

passwords and operating instructions. These manuals often appear on the internet and can aid malicious actors in conducting cyberattacks on industrial control systems.

Researchers and federal agencies have recently identified concerns about the potential introduction of cyber vulnerabilities to the grid through the connection of consumer IoT devices to the grid's distribution network. For example, university researchers in 2018 used large, real-world grid models to simulate the feasibility and impact on the grid of a coordinated cyberattack on smart home appliances.⁵² Specifically, the researchers found that malicious threat actors could compromise a large number of high-wattage IoT devices (e.g., air conditioners and heaters) and turn them into a botnet—a network of devices infected with malicious software and controlled as a group without the owners' knowledge.⁵³

The malicious actors could then use the botnet to launch a coordinated attack aimed at manipulating the demand across distribution grids. For example, according to the researchers, one such attack could involve synchronously switching on all of the compromised devices. Such an attack could disrupt the balance of power generation and consumption and ultimately cause an outage.

An official from the National Renewable Energy Laboratory explained that the likelihood of attacks on the distribution network using IoT devices is low but could increase in the future. In particular, the official explained that the wattage needed to create a significant disruption in the balance of supply and demand would require a botnet of tens of thousands of smart appliances. Botnets of this size have been created,⁵⁴ but the laboratory official explained that it would be very difficult to manipulate all of those devices to turn on at precisely the same time. However, the official cautioned that such an attack could become more plausible in the future

⁵²S. Soltan, P. Mittal, and H.V. Poor, *BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid*, 27th USENIX Security Symposium, Baltimore, MD, August 15 – 17, 2018.

⁵³The official at the National Renewable Energy Laboratory suggested that a vulnerability introduced into the firmware distributed by a vendor could plausibly be exploited by a malicious actor's malware to create a botnet of smart appliances.

⁵⁴According to a DHS alert, the purported Mirai botnet author claimed that over 380,000 IoT devices were enslaved by the Mirai malware. Department of Homeland Security, *Heightened DDoS Threat Posed by Mirai and Other Botnets*, Alert TA16-288A (Washington, D.C.: Last revised October 17, 2017).

Global Positioning System
Vulnerability

as additional high-wattage systems and devices, such as building energy management systems and electric vehicles, are connected to the internet.

The grid is dependent on GPS timing to monitor and control generation, transmission, and distribution functions. According to DOE, the GPS signal is susceptible to exploitation by malicious actors. For example, a malicious actor could inject a counterfeit GPS signal (known as GPS spoofing) that could result in disruptions to grid operations.

U.S. Cybersecurity
Incidents Reportedly Have
Not Caused Power
Outages, and the Potential
Impacts from a
Cyberattack Are Uncertain

According to the three entities responsible for collecting information on cybersecurity incidents that affect the electric grid—DHS, DOE, and NERC—none of the cybersecurity incidents reported in the United States have disrupted the reliability or availability of the grid, and none have resulted in a power outage.⁵⁵

Even though cyber incidents involving the grid reportedly have not caused power outages in the United States, cyberattacks on foreign industrial control systems have resulted in power outages. For example, in December 2015, malicious actors linked by Ukrainian officials to the Russian government conducted cyberattacks on three Ukrainian power distribution operators, resulting in a loss of power for about 225,000 customers.⁵⁶ GAO did not find evidence that these attacks physically damaged grid components, but cyberattacks on industrial control systems in other sectors demonstrates that this is possible. For example, in 2014, malicious cyber actors compromised industrial control systems and caused failures that led to massive damage to a blast furnace at a German steel mill.

Further, federal agencies have performed three assessments of the potential impacts of cyberattacks on the industrial control systems supporting the grid. Specifically, DOE and FERC have conducted three

⁵⁵From 2014 through 2018, grid owners and operators reported 17 events to DOE that were initially believed to be caused by cyber-related activity. However, according to DOE, after further analysis of the 17 events, only four were determined to be related to cybersecurity, and none disrupted the reliability or availability of the grid or resulted in a power outage.

⁵⁶Department of Homeland Security, Industrial Control Systems, *Cyber-Attack Against Ukrainian Critical Infrastructure*, IR-ALERT-H-16-056-01 (Aug. 23, 2018 [revised]). The press reported that cyberattacks in December 2016 used advanced malware to target an electric power transmission system in the Ukrainian capital, Kiev, which resulted in a power outage of one-fifth of a gigawatt.

assessments of the potential impact of cyberattacks on the grid at the scale of multiple system operators through the scale of an interconnection. The two DOE assessments—which according to DOE officials are early drafts and have not gone through intra-agency review—focused on the impact of a cyberattack within a single interconnection and produced varying reports of the potential scale of power outages that could result from a cyberattack.⁵⁷ The remaining assessment—which FERC conducted in 2013—reviewed the impact of a cyber or physical attack on all three interconnections and concluded that an attack could result in a widespread blackout spanning the contiguous United States. Table 1 below describes the three assessments.

Table 1: Federal Assessments of Cyberattacks and Electric Grid Operation Impacts of National Significance

Federal Assessment	Year	Scope	Scale of power outage
Federal Energy Regulatory Commission (FERC), <i>Identifying Electrically Significant Locations on the Bulk Power System</i>	2013	All three interconnections	The assessment assumed that attackers disabled power availability at key substations. According to FERC's assessment, a loss of a small number of specific generators or substations in each interconnection could result in a widespread blackout.
Argonne National Laboratory, <i>Analysis of Electricity Transfer Capabilities among Region V Regional Transmission Organizations^a</i>	2017	Eastern Interconnection—specifically, Federal Emergency Management Agency Region V, which covers six states and spans three North American Electric Reliability Corporation regions	The assessment assumed that multiple power plants were damaged and removed from service by a cyberattack, resulting in the abrupt loss of significant generating capacity. The sudden loss of generation would cause a large portion of the Eastern Interconnection to collapse, resulting in outages in various parts of the grid. Specifically, the draft assessment identified that most of the Federal Emergency Management Agency region's electricity demand would be unserved, resulting in widespread outages across much of the six-state region.

⁵⁷ DOE reported on the results of one of these two draft assessments—the 2017 edition of the *Electricity Subsector Risk Characterization Study*—in its 2017 *Assessment of Electricity Disruption Incident Capabilities*, which was developed in response to Executive Order 13800. The other draft assessment was conducted by DOE's Argonne National Laboratory for the Federal Emergency Management Agency.

Federal Assessment	Year	Scope	Scale of power outage
Department of Energy (DOE), Office of Infrastructure Security and Energy Restoration, <i>Electricity Subsector Risk Characterization Study</i> ^a	2017, 2018, 2019	Western Interconnection	The first annual draft assessment in 2017 evaluated three cyberattack scenarios and assumed a worst-case scenario of a loss of multiple gigawatts. The 2017 draft assessment concluded that a cyberattack resulting in the loss of a relatively small amount of gigawatts could occur with a likelihood of about eight times per year, while the loss of a more substantial amount of gigawatts had a likelihood of occurring about once in 100 years. DOE's 2018 draft assessment evaluated seven cyberattack scenarios and revised its estimate to be that the loss of the more substantial amount of gigawatts had increased to an average likelihood of occurring nearly once every 10 years. DOE's 2019 draft assessment maintained the same seven attack scenarios and concluded that the loss of the more substantial amount of gigawatts had an average likelihood of occurring about once in 100 years, while the loss of the relatively small amount of gigawatts decreased to about once every 2 years.

Source: GAO analysis of agency documents. | GAO-19-332

^aAccording to DOE officials, this assessment is an early draft that has not gone through intra-agency review.

However, because of limitations in the three federal assessments, the scale of any power outages that may result from a cyberattack is uncertain. In particular:

- Federal agencies have conducted one study—FERC's 2013 study—that assesses the potential impact of a coordinated attack in each of the three interconnections. However, in 2015, DOE officials raised concerns about the scenario and related assumptions used in that study that called into question the findings. Specifically, at that time, DOE officials reported that they found several of the scenario's assumptions highly unlikely, including peak capabilities at all targeted generation stations at the time of an attack and the loss of all safety systems designed to prevent the consequences described in the analysis. Further, DOE officials reported that they found the study's scenarios even more unlikely to result in a total loss of power or any other consequence that could be reasonably expected to result in damage to national security.⁵⁸
- The 2017 assessment conducted by DOE's Argonne National Laboratory was limited in scope to a six-state region. In addition, the

⁵⁸According to DOE officials, DOE's current position is that the study's assumptions, methodology, and findings were accurate for their intended purpose, and DOE is considering them in the context of its current analyses.

assessment focused on a single cyberattack scenario and noted that many other grid cyberattack methods and outcomes were possible.

- The 2017, 2018, and 2019 editions of DOE's draft *Electricity Subsector Risk Characterization Study* have significant methodological limitations. Specifically, officials from Lawrence Livermore National Laboratory who were contracted to perform the analyses cautioned that they used a reduced model of the Western Interconnection as it existed around 1980 and emphasized that their methodology should not be used to predict the behavior of the actual bulk power system. For example, those researchers told us that their selected model of the Western Interconnection had less than a quarter of its actual capacity in 2018.

The DOE official responsible for the studies said that the assumption for the worst-case scenario was from that official's professional judgement, not a documented analysis. Later, officials at Sandia National Laboratories told us that the worst-case scenario in the DOE draft study was a point solution used as a proof of concept, that the study was not of a high level of rigor, and that the assumptions may not represent a vulnerability in the actual bulk power system. Further, the DOE methodology assumed that all assets removed from service were treated equally; accordingly, the researchers did not distinguish the loss of specific assets (such as a substation or transmission line) in the calculation of attack difficulty and likelihood.

Because of these limitations, some of the draft studies' conclusions may not be realistic. For example, one of DOE's major conclusions in the 2017 *Risk Characterization Study*—that a cyberattack may result in a relatively small loss of load in the United States about 8 times per year—may not be plausible because there have not been any reported cyberattacks that have caused an outage in the United States.⁵⁹ In addition, the three draft DOE studies have widely varying conclusions on the likelihood of cyberattacks across the selected range of loss of load. For example, the 2018 draft study concluded that a cyberattack resulting in a more substantial loss of load had an average likelihood of occurring nearly once every 10 years, while the 2019 draft study concluded that such an attack would occur about once every 100 years. According to a DOE official, there is no documentation of the technical basis for the significant changes in the

⁵⁹Further, the likelihood of such a loss decreased by more than a factor of 10 between the 2017 and 2019 draft reports.

assessment outcomes between the 2017 and 2018 draft studies and between the 2018 and 2019 draft studies. In addition, DOE officials told us that all three studies are early drafts and have not gone through intra-agency review.⁶⁰

Moreover, none of the federal assessments reviewed the risk associated with a cyberattack involving a botnet of high-wattage consumer IoT devices. As previously mentioned, university researchers demonstrated that malicious actors could use a botnet of IoT devices to launch a coordinated attack aimed at manipulating the demand on distribution systems across the grid. A federal official we interviewed agreed that such an attack could occur and could disrupt grid distribution systems—especially as additional high-wattage systems become connected to the internet—but they said it is unclear what impact, if any, such attacks could have on the reliability of the bulk power system.

Grid Entities Reported Facing Challenges in Addressing Cybersecurity Risks

Officials and representatives of key federal and nonfederal entities we interviewed generally identified five significant challenges grid owners and operators face in addressing cybersecurity risks: (1) difficulties in hiring a sufficient cybersecurity workforce, (2) limited public-private information sharing of classified information, (3) limited resources to invest in cybersecurity protections, (4) reliance on other critical infrastructure that may be vulnerable to cyberattacks, and (5) uncertainties about how to implement cybersecurity standards and guidance.

Hiring a Sufficient Cybersecurity Workforce

Officials and representatives of key federal and nonfederal entities we interviewed identified difficulties in hiring a sufficient cybersecurity workforce as a significant challenge to addressing cybersecurity risks to the grid. For example, a representative of a nonfederal entity told us that there are a limited number of trained cybersecurity personnel interested in working in the energy sector. The representative added that there are a large number of vacancies for cybersecurity positions and that they are difficult to fill due to the limited amount of available talent and organizational resource constraints, such as providing salaries that are competitive with other sectors. A laboratory official commented that larger grid entities are able to attract the majority of skilled cybersecurity professionals, leaving smaller entities with less skilled personnel. Further,

⁶⁰DOE reported on the results of the 2017 draft study in its 2017 *Assessment of Electricity Disruption Incident Capabilities*, which was developed in response to Executive Order 13800.

an asset owner explained that training personnel so that they have sufficient cybersecurity knowledge and skills is difficult, and the requisite knowledge of industrial control systems further complicates training these personnel.

DOE has also identified difficulties in hiring a sufficient cybersecurity workforce as a challenge. Specifically, according to DOE's *Assessment of Electricity Disruption Incident Response Capabilities*, the electricity subsector continues to face challenges in recruiting and maintaining experts with strong knowledge of cybersecurity practices as well as knowledge of industrial control systems supporting the grid.

Limited Public-Private Sharing of Classified Information

Officials and representatives of key federal and nonfederal entities we interviewed identified limited public-private sharing of classified information, including the sharing of threat intelligence, as a significant challenge to addressing cybersecurity risks to the grid. For example, a laboratory official told us that many grid owners and operators do not have security clearances. Consequently, the official explained, deeming information on certain cybersecurity threats to the grid to be "classified" leaves many utilities without the awareness to address those threats to the grid. The official added that when details are removed from classified threat intelligence in order to develop an unclassified alert, that alert often lacks the specific information utilities need to address the threat.

Asset owners told us that, even for those grid owners and operators who are permitted to initiate the clearance process, it can take an extended period of time to complete the associated adjudication to obtain that clearance. In addition, two asset owners noted that, even after clearances have been received and fully adjudicated, it is often difficult to obtain access to secure locations to review classified information.

DOE has also identified limited public-private information sharing as a challenge. Specifically, according to DOE's *Assessment of Electricity Disruption Incident Response Capabilities*, the bidirectional flow of information and intelligence between industry and government has been highlighted by stakeholders as a continued challenge for the electricity subsector. The assessment explains that the sharing of information is impeded by the slow adoption of automated capabilities and the difficulty of sharing classified information between government and industry—particularly in real time during an incident.

Limited Resources to Invest in Cybersecurity Protections

Officials and representatives of key federal and nonfederal entities identified limited resources for cybersecurity protections as a challenge to

Reliance on Other Critical Infrastructure That May Be Vulnerable to Cyberattacks

addressing cybersecurity risks to the grid. In particular, most of the asset owners that we met with stated that it can be costly to implement required cybersecurity protections. In addition, officials and representatives of key federal and nonfederal entities that we spoke with explained that costs—including those for cybersecurity protections—must be recovered through electric rates to customers. As a result, a laboratory official explained that many utilities prioritize cybersecurity protections that are the most cost-effective over protections that may be needed to address risks.

Officials and representatives of key federal nonfederal entities we interviewed identified the grid's reliance on other critical infrastructure (e.g., natural gas pipelines) that may be vulnerable to cyberattacks as a challenge to addressing cybersecurity risks to the grid.⁶¹ For example, a representative of a nonfederal entity stated that the electricity subsector inherits cybersecurity risks from other critical infrastructures, since the electricity subsector relies on those critical infrastructures for its own operations. As such, that representative added that it is difficult to holistically determine how vulnerable the grid may be to a cyberattack. In addition, as previously mentioned, according to the 2019 *Worldwide Threat Assessment*, China has the ability to disrupt a natural gas pipeline for days to weeks.

Uncertainties about Implementation of Cybersecurity Standards and Guidance

Officials and representatives of key federal and nonfederal entities we interviewed identified uncertainties about how to implement cybersecurity standards and guidance as a challenge to addressing cybersecurity risks to the grid. In particular, several representatives noted that these uncertainties have led their organizations to devote additional resources to implementing the standards and guidance. For example, one asset owner explained that FERC-approved cybersecurity standards do not always include details that are needed to understand how they apply to that owner's environment. In addition, another asset owner stated that significant time and effort is required to understand the standards and how they might be implemented.

⁶¹In December 2018, we reported that pipelines used to transport natural gas—the largest source of U.S. electricity generation in 2018, accounting for about 35 percent of the nation's electricity—are vulnerable to cyberattacks. GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, [GAO-19-48](#) (Washington, D.C.: Dec. 19, 2018).

Federal Agencies Have Performed a Variety of Activities Aimed at Addressing Grid Cybersecurity Risks

DOE, DHS, and other federal agencies have performed a variety of critical infrastructure protection activities aimed at addressing grid cybersecurity risks, including implementing programs that help protect grid systems from cybersecurity threats and vulnerabilities. In addition, FERC has performed a variety of regulatory activities aimed at addressing grid cybersecurity risks, such as approving mandatory cybersecurity standards for the bulk power system.

DOE, DHS, and Other Agencies Have Undertaken Critical Infrastructure Protection Activities Aimed at Addressing Grid Cybersecurity Risks

DOE, DHS, and other federal agencies have performed a variety of critical infrastructure protection activities aimed at addressing grid cybersecurity risks. These activities generally align with the functions in the NIST Cybersecurity Framework, which include (1) protecting systems to mitigate cybersecurity threats and vulnerabilities; (2) identifying cybersecurity threats and vulnerabilities and detecting potential cybersecurity incidents; and (3) responding to and recovering from such incidents.⁶²

Protecting systems to mitigate cybersecurity threats and vulnerabilities

Federal agencies assist grid asset owners and operators in implementing protections that mitigate cybersecurity risks by providing capabilities aimed at preventing cybersecurity intrusions and offering training and guidance on cybersecurity practices. For example, DHS's Enhanced Cybersecurity Services program provides intrusion-prevention capabilities to U.S.-based entities and to state, local, tribal, and territorial organizations. To carry out this voluntary program, DHS provides classified and unclassified threat information to designated commercial service providers. These providers use the information to block access to (1) specific malicious internet addresses and (2) email with specific malicious criteria.

NIST, DHS, and DOE also provide cybersecurity training and guidance. For example, NIST has developed numerous special publications on cybersecurity protections for IT and industrial control systems, such as the previously mentioned *Cybersecurity Framework* and its *Guide to*

⁶²National Institute of Standards and Technology, *Cybersecurity Framework*.

Industrial Control Systems.⁶³ In addition, DHS provides in-person and online training on leading cybersecurity practices for industrial control systems through its National Cybersecurity and Communications Integration Center.

Lastly, DHS has taken initial steps to help grid entities manage supply chain cybersecurity risks. For example, in July 2018 DHS created a public-private partnership, known as the Supply Chain Risk Management Task Force. The task force aims to examine risks to the global information and communications technology supply chain and develop consensus recommendations to manage such risks.

Identifying cybersecurity threats and vulnerabilities and detecting potential cybersecurity incidents

Federal agencies help grid entities identify cybersecurity risks and detect incidents by providing threat and vulnerability information, performing risk assessments, performing forensic analysis, and conducting research. For example, DOE piloted and launched the Cybersecurity Risk Information Sharing Program, which is now managed by the Electricity Information Sharing and Analysis Center. It provides a voluntary, bi-directional public-private IT data sharing and analysis platform. Using both classified and unclassified sources, DOE's Pacific Northwest National Laboratory analyzes the information to (1) identify threat patterns and attack indicators, and (2) deliver alerts to owners and operators. In addition, DHS's Automated Indicator Sharing program provides a server housed at each participant's location that can be used to exchange threat indicators with the department's National Cybersecurity and Communications Integration Center. Further, the center provides asset owners with alerts, advisories, and situational reports, including information on threats, vulnerabilities, or activity that could affect IT or industrial control system networks.

DOE and DHS also offer services aimed at helping grid owners and operators assess cybersecurity risks and perform forensic analysis. For example, DOE has an evaluation tool known as the Electricity Cybersecurity Capability Maturity Model that aims to help the electricity

⁶³National Institute of Standards and Technology, *Cybersecurity Framework and Guide to Industrial Control Systems (ICS) Security*, NIST 800-62 Rev. 2 (Gaithersburg, MD: May 2015).

industry evaluate, prioritize, and improve its cybersecurity capabilities.⁶⁴ In addition, DHS offers technical assessments through its National Cybersecurity and Assessment and Technical Services Team that can help identify vulnerabilities and simulate a malicious adversary. Further, DHS can review potential cybersecurity incident artifacts, such as malware, phishing emails, and network logs, at its National Cybersecurity and Communications Integration Center to determine the existence or extent of a cybersecurity threat or incident.

Moreover, DOE's Cybersecurity for Energy Delivery Systems program sponsors grid cybersecurity research through DOE's national laboratories. For example:

- Oak Ridge National Laboratory has conducted research on mechanisms that could help critical infrastructure entities better detect vulnerabilities in software used in industrial control systems.
- Four national laboratories have engaged in a project that aims to improve the capability of grid entities to collect and analyze data from their industrial control system networks and detect cybersecurity incidents.⁶⁵
- Oak Ridge National Laboratory and Pacific Northwest National Laboratory have a joint project to develop mechanisms for more quickly detecting and eradicating malware on industrial control systems.

Responding to and recovering from cybersecurity incidents

Federal agencies have developed policies, strategies, and plans to define their roles and responsibilities for responding to and recovering from grid cybersecurity incidents. In particular, DHS has responsibility for leading the federal effort to mitigate or lessen the impact of such incidents, the Department of Justice has responsibility for the federal law enforcement response to the threats, and DOE has authority, in designated emergencies, to impose measures to restore the reliability of critical

⁶⁴As another example, DHS offers two checklist-based risk assessments—the Cyber Resilience Review and the Cybersecurity Evaluation Tool—to evaluate IT and industrial control system cybersecurity practices.

⁶⁵The four national laboratories engaged in the pilot are Idaho National Laboratory, Argonne National Laboratory, Oak Ridge National Laboratory, and Pacific Northwest National Laboratory.

electric infrastructure. DOE is also responsible for coordinating the energy sector-specific response with DHS and the Department of Justice.⁶⁶

Federal agencies have also taken steps to help prepare asset owners for cyber response and recovery efforts. For instance, DHS has worked with nonfederal entities to simulate response and recovery efforts to a cyberattack through exercises such as Cyber Storm.⁶⁷ In addition, DOE, in conjunction with the National Association of State Energy Officials, has conducted regional energy assurance exercises. These exercises aim to promote state and local preparedness and resilience for future energy emergencies stemming from a cyber incident.

FERC Has Performed Regulatory Activities Aimed at Addressing Grid Cybersecurity Risks

FERC has performed a variety of regulatory activities aimed at addressing grid cybersecurity risks. These activities include (1) approving mandatory cybersecurity standards for the bulk power system, (2) enforcing regulatory requirements through imposition of civil penalties, (3) auditing the performance of the electric reliability organization—NERC—and its regional entities, and (4) auditing bulk power entities for compliance with the mandatory cybersecurity standards.

- **Approve mandatory cybersecurity standards.** FERC has approved mandatory reliability standards relating to cybersecurity protections. For example, in October 2018, FERC approved a new standard to bolster supply chain risk management protections for the nation’s bulk electric system. This new standard, which will become enforceable in July 2020, is intended to augment existing standards that aim to mitigate cybersecurity risks associated with the supply chain for grid-related cyber systems.
- **Enforce regulatory requirements through imposition of civil penalties.** FERC has referred violations of its approved cybersecurity

⁶⁶Department of Homeland Security, *National Cyber Incident Response Plan*, (December 2016)

⁶⁷According to DHS, Cyber Storm participants perform the following activities: (1) examine organizations’ capability to prepare for, protect from, and respond to the potential effects of cyberattacks; (2) exercise strategic decision-making and interagency coordination of incident response(s) in accordance with national-level policy and procedures; (3) validate information-sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response, and recovery information; and (4) examine means and processes through which to share sensitive information across boundaries and sectors without compromising proprietary or national security interests.

standards to NERC to impose penalties on the bulk power entities that committed the violations.⁶⁸ For example, such a notification occurred in January 2019 when NERC assessed a \$10 million penalty based on 127 violations of the cybersecurity standards made by an undisclosed entity.

- **Audit the performance of the electric reliability organization.** FERC has audited NERC's performance as the electric reliability organization. In this audit, which it completed in 2012, FERC evaluated NERC's budget formulation, administration, and execution. With respect to cybersecurity, FERC recommended that NERC (1) assess its existing staffing levels to ensure adequate resources to accomplish critical infrastructure protection work related to cybersecurity and (2) devote greater resources to carrying out its oversight duties. In 2013, FERC closed these recommendations after reviewing NERC's plans for evaluating its staffing levels and its commitment to add resources in its business plan. According to FERC officials, FERC continues to monitor the level of resources NERC devotes to cybersecurity oversight through its annual review of NERC's budget
- **Audit bulk power entities for compliance with standards.** FERC has audited bulk power entities' compliance with its approved cybersecurity standards. From 2016 through 2018, FERC conducted its own independent audits of eight bulk power entities for compliance with those standards and produced public lessons learned reports based on the results. According to FERC officials, the agency plans to conduct four such audits every fiscal year starting in fiscal year 2019 and to continue producing annual lessons learned reports based on the results. In addition, since the first of the cybersecurity standards became enforceable in 2009, FERC has observed eight NERC regional entity-led audits a year—one in each NERC region—focused on bulk power entity compliance with those standards.⁶⁹

⁶⁸FERC has the authority to impose penalties on noncompliant bulk power entities for violations of the approved NERC standards. In practice, FERC has referred violations to NERC to investigate and, if warranted, penalize bulk power entities that did not comply with the mandatory cybersecurity standards.

⁶⁹There are seven NERC regions, each with a regional entity to which NERC has delegated its authority to monitor and enforce compliance with reliability standards. There were eight regions until 2017, when NERC dissolved one of the regional entities and transferred its responsibilities to other regional entities.

DOE Has Not Fully Defined a Strategy to Address Grid Cybersecurity Risks and Challenges

National strategies are critical tools used to help address longstanding and emerging issues that affect national security and economic stability. In 2004, we identified a set of desirable characteristics for effective national strategies.⁷⁰ These characteristics include:⁷¹

- **Purpose, scope, and methodology.** Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed.
- **Problem definition and risk assessment.** Addresses the particular national problems, assesses the risks to critical assets and operations—including the threats to, and vulnerabilities of, critical operations—and discusses the quality of data available regarding the risk assessment.
- **Goals, subordinate objectives, activities, and performance measures.** Addresses what the strategy is trying to achieve; steps to achieve those results; and the priorities, milestones, and performance measures that include measurable targets to gauge results and help ensure accountability.
- **Discussion of needed resources and investments.** Addresses what the strategy will cost and the types of resources and investments needed.
- **Organizational roles, responsibilities, and coordination.** Addresses who will implement the strategy, what their roles will be, and mechanisms to coordinate their efforts.

As previously noted, the executive branch has taken steps toward outlining a federal strategy for confronting cyber threats—including threats to critical infrastructure such as the grid. In addition, as the sector-specific agency, DOE has led the development of approaches to implement the federal cybersecurity strategy for the energy sector, including the grid. Table 2 identifies and describes these approaches—specifically, two agency plans and an assessment—for addressing grid cybersecurity risks and challenges.

⁷⁰[GAO-04-408T](#).

⁷¹We did not assess the characteristic of integration and implementation because it is not applicable to implementation plans for an overarching national strategy.

Table 2: DOE Plans and Assessment Addressing Electric Grid Cybersecurity Risks and Challenges

Initiative	Year of issuance	Description
Department of Energy (DOE) and Department of Homeland Security (DHS) <i>Energy Sector-Specific Plan</i>	2015	This plan helps guide and integrate efforts to improve the security and resilience of the energy sector’s critical infrastructure, including the electric grid. The plan identifies three federal priorities for enhancing the security and resilience of the grid: (1) deploying tools and technologies to enhance awareness of potential disruptions, (2) planning and exercising coordinated responses to disruptive events, and (3) ensuring actionable intelligence on threats is communicated between government and industry in a time-sensitive manner.
DOE and DHS <i>Assessment of Electricity Disruption Incident Response Capabilities</i>	2017	Developed in response to Executive Order 13800, the assessment examines the potential scope and duration of a prolonged power outage associated with a significant cyber incident. Relying on DOE’s draft 2017 DOE Electricity Subsector Risk Characterization Study, the assessment characterizes the potential range of load loss resulting from four cyberattack scenarios. The assessment also evaluates the readiness and gaps in the United States’ ability to manage and mitigate consequences of a cyber incident against the electric subsector.
DOE <i>Multiyear Plan for Energy Sector Cybersecurity</i>	2018	This plan 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. It identifies the goals, objectives, and activities that DOE will pursue over the next 5 years to reduce the risk of energy disruptions from cyber incidents. It also describes how DOE will carry out its mandated cybersecurity responsibilities and address the evolving security needs of energy owners and operators.

Source: GAO analysis of federal plans and assessment. | GAO-19-332

The two plans and the assessment do not fully address all of the key characteristics needed for a national strategy. Collectively, the plans and assessment fully address one characteristic—purpose, scope, and methodology—and partially address the other four characteristics of a national strategy (see table 3).

Table 3: Extent to Which DOE Grid Cybersecurity Plans and Assessment Address the Key Characteristics of a National Strategy

Characteristic	Department of Energy (DOE) and Department of Homeland Security (DHS) <i>Energy Sector-Specific Plan</i>	DOE and DHS <i>Assessment Of Electricity Disruption Incident Response Capabilities</i>	DOE <i>Multiyear Plan for Energy Sector Cybersecurity</i>
Purpose, scope, and methodology	●	●	●
Problem definition and risk assessment	◐	◐	◐
Goals, subordinate objectives, activities, and performance measures	◐	N/A	◐
Resources and investments	◐	N/A	◐
Roles, responsibilities, and coordination	◐	N/A	◐

Legend: ●—Fully addresses all aspects of the characteristic. ◐—Partially addresses some but not all of the characteristic. ○—Does not address any aspects of the characteristic. N/A – This characteristic is not applicable because DOE’s and DHS’s *Assessment of Electricity Disruption Incident Response Capabilities* was not intended to outline goals, objectives, activities, and performance measures; resources and investments; and roles, responsibilities, and coordination.

Source: GAO analysis of federal plans and assessment. | GAO-19-332

Purpose, scope, and methodology

The plans and assessment fully address the characteristic of outlining their purpose, scope, and methodology. For example, the *Energy Sector-Specific Plan* explains that it was produced to help integrate and guide the sector's continuing effort to improve the security and resilience of critical infrastructure. In addition, the plan explains that DOE worked closely with the Energy Sector Coordinating Council and the Energy Sector Government Coordinating Council, among others, to develop the plan.

Problem definition and risk assessment

The plans and the assessment partially address the characteristic of defining the problem and performing a risk assessment. Each defines the problems that it was intended to address and assesses cybersecurity risks to the grid. For example, DOE's *Assessment of Electricity Disruption Incident Response Capabilities* states that it was developed in response to Executive Order 13800's requirement that DOE examine the potential scope and duration of a prolonged power outage associated with a significant cyber incident. In addition, as previously mentioned, the assessment describes the potential range of load loss resulting from four cyberattack scenarios.⁷²

However, the discussion of the quality of data available regarding DOE's assessment is inaccurate. According to the assessment, the potential range of load loss resulting from four cyberattack scenarios was based on rigorous modeling and analysis from multiple DOE national laboratory experts. However, these results were based on the 2017 *Electricity Subsector Risk Characterization Study*, which as previously described, has significant limitations affecting the quality of data.

In addition, neither the plans nor the assessment fully analyzed the cybersecurity risks and challenges to the grid. In particular, none of them analyzed the threat of, and vulnerabilities to, a cyberattack spanning all three interconnections. In addition, the initiatives did not assess the vulnerability of the grid to a cyberattack involving high-wattage consumer IoT devices connected to the grid's distribution system.

⁷²DOE's *Assessment of Electricity Disruption Incident Response Capabilities* references DOE's draft 2017 *Electricity Subsector Risk Characterization Study*.

Goals, subordinate objectives, activities and performance measures

The two plans partially address the characteristic of outlining goals, subordinate objectives, activities, priorities, milestones, and performance measures.⁷³ Both plans outline the goals, objectives, and activities for addressing cybersecurity risks facing the electric grid. For example, the *Energy Sector-Specific Plan* describes five goals for the energy sector and three related priorities for the electricity subsector. However, the plans' goals, objectives, and activities do not fully address the cybersecurity risks to the grid. For example, neither plan includes goals and activities that address the vulnerability of the grid to a cyberattack involving high-wattage consumer IoT devices connected to the grid's distribution system. Further, in light of the previously identified gaps in the analysis of cybersecurity risks and challenges, the plans' goals, objectives, and activities are likely not commensurate with grid cybersecurity risks and challenges.

Moreover, only one of the plans—DOE's *Multiyear Plan for Energy Sector Cybersecurity*—includes milestones and performance measures for achieving the goals, objectives, and activities. Additionally, this plan does not include performance measures with measurable targets for all objectives, including those aimed at providing timely cyber threat briefings to energy sector partners and developing cyber incident response processes and procedures.

Resources and investments

The two plans partially address the characteristic of describing resource and investment needs.⁷⁴ Specifically, although the plans identify many resources and investments needed to achieve their goals and objectives, they do not fully identify resource and investment needs. For example, one of the objectives of DOE's *Multiyear Plan for Energy Sector Cybersecurity* is to establish a coordinated national cyber incident response capability for the energy sector. However, the plan does not describe the resources or investments needed to meet this objective. This

⁷³DOE's *Assessment of Electricity Disruption Incident Response Capabilities* was not intended to outline goals, objectives, and performance measures. Therefore, this characteristic is not applicable to this assessment.

⁷⁴DOE's *Assessment of Electricity Disruption Incident Response Capabilities* was not intended to describe resource and investment needs. Therefore, this characteristic is not applicable to this assessment.

is of particular concern because, as previously mentioned, the Fixing America's Surface Transportation Act of 2015 authorized DOE to order emergency measures, following a Presidential declaration of a grid security emergency, to protect or restore the reliability of critical electric infrastructure.

In addition, the plans do not describe specific investment costs associated with carrying them out. For example, DOE's *Multiyear Plan for Energy Sector Cybersecurity* describes the need to develop a laboratory for identifying and analyzing cybersecurity vulnerabilities to energy delivery systems. However, the plan does not identify the specific costs associated with this investment. Further, given the previously discussed gaps in risk analysis, goals, and objectives, it is unclear to what extent the identified resources and investment needs are sufficient to address electric grid cybersecurity risks and challenges.

Roles, responsibilities, and coordination

The two plans partially address the characteristic of describing roles, responsibilities, and coordination mechanisms for carrying out the goals, objectives, and activities.⁷⁵ Specifically, the plans describe mechanisms for coordinating but do not always identify organizations responsible for achieving the goals, objectives, and activities. For example, DOE's *Multiyear Plan for Energy Sector Cybersecurity* states that the department will partner with DOE's national laboratories to carry out several activities in the plan. However, the plan does not indicate which of the 10 national laboratories DOE will partner with for each activity.

In a written response, DOE explained that executive branch documents that outline the broader federal strategy for confronting cyber threats—such as the *National Cyber Strategy* and the *DHS Cybersecurity Strategy*—address the key characteristics of a national strategy not addressed in DOE's plans and assessment. In addition, DOE stated that the department's plans and assessment for addressing risks and challenges facing the grid support and fit within the context of that broader cybersecurity framework while allowing the agency flexibility to accomplish its goals.

⁷⁵DOE's *Assessment of Electricity Disruption Incident Response Capabilities* was not intended to describe roles, responsibilities, and coordination. Therefore, this characteristic is not applicable to this assessment.

Although the broader executive branch strategy documents on confronting cyber threats provide a framework for addressing critical infrastructure cybersecurity risks and challenges, they do not address the specific risks and challenges facing the electric grid. In addition, as previously mentioned, we have reported that these broader executive branch strategy documents also do not include key characteristics of a national strategy.⁷⁶ Until DOE ensures it has a plan aimed at implementing the federal cybersecurity strategy relating to the grid that addresses all of the key characteristics of a national strategy—including a full assessment of cybersecurity risks—the guidance the plan provides decision makers in allocating resources to address risks and challenges will likely be limited.

FERC-Approved Standards Do Not Fully Address Grid Cybersecurity Risks

FERC has not ensured that its approved grid cybersecurity standards fully address leading federal guidance for improving critical infrastructure cybersecurity—specifically, the NIST Cybersecurity Framework. In addition, FERC has not evaluated the risk of a coordinated cyberattack on geographically distributed targets in approving the threshold for which grid cyber systems must comply with requirements in the full set of grid cybersecurity standards.

FERC-Approved Standards Do Not Fully Address Leading Federal Guidance for Improving Critical Infrastructure Cybersecurity

The NIST Cybersecurity Framework provides a set of cybersecurity activities, desired outcomes, and applicable references that are common across all critical infrastructure sectors. The framework also states that while it is not exhaustive, it is capable of being extended, allowing organizations, sectors, and other entities to use references that are most appropriate to enable them to manage their cybersecurity risk. NIST recommends that organizations use the Cybersecurity Framework functions, categories, and subcategories to identify the key controls needed to meet their security objectives (see Table 4 for the functions and categories).

⁷⁶[GAO-18-622](#) and [GAO-19-157SP](#).

Table 4: National Institute of Standards and Technology (NIST) Cybersecurity Framework Functions and Categories

Function	Category
Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities	Asset management
	Business environment
	Governance
	Risk assessment
	Risk management strategy
	Supply chain risk management
Protect: Develop and implement appropriate safeguards to ensure delivery of critical services	Identity management, authentication and access control
	Awareness and training
	Data security
	Information protection processes and procedures
	Maintenance
	Protective technology
Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event	Anomalies and events
	Security continuous monitoring
	Detection processes
Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event	Response planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	Recovery planning
	Improvements
	Communications

Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity. | GAO-19-332

To promote widespread adoption of the framework, Executive Order 13636 called for sector-specific agencies to develop mechanisms to encourage the framework’s adoption. In addition, the order called for regulatory agencies to review the framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks.

However, the FERC-approved cybersecurity standards do not fully address the NIST Cybersecurity Framework’s five functions and associated categories and subcategories. More specifically, the

cybersecurity standards substantially address two of the five functions and partially address the remaining three functions. Table 5 depicts the extent to which these standards address the framework’s five functions and 23 categories. (Appendix II contains more detailed information regarding the extent to which the standards address the framework’s 108 subcategories.)

Table 5: Extent to Which Federal Energy Regulatory Commission-Approved Cybersecurity Standards Address NIST Cybersecurity Framework Functions and Categories

Function	GAO assessment	Category	GAO assessment
Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	●	Asset management	●
		Business environment	○
		Governance	●
		Risk assessment	●
		Risk management strategy	○
		Supply chain risk management	●
Protect: Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.	●	Identity management, authentication, and access control	●
		Awareness and training	●
		Data security	●
		Information protection processes and procedures	●
		Maintenance	●
		Protective technology	●
Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	●	Anomalies and events	●
		Security continuous monitoring	●
		Detection processes	●
Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity event.	●	Response planning	●
		Communications	●
		Analysis	●
		Mitigation	●
		Improvements	●
Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	●	Recovery planning	●
		Improvements	●
		Communications	○

Legend: ●—Fully address: the standards address all of the related subcategories. ●—Substantially address: the standards address at least two-thirds, but not all, of the related subcategories. ●—Partially address: the standards address at least one-third, but less than two-thirds, of the related subcategories. ●—Minimally address: the standards address less than one-third of the related subcategories. ○—Do not address: the standards do not address any of the related subcategories.

Source: GAO analysis of North American Electricity Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards in comparison with functional areas in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. | GAO-19-332

As shown in table 5, the FERC-approved cybersecurity standards either fully address or substantially address eight of the 23 categories. For example:

- The standards fully address the identity management, authentication, and access control category by fully addressing seven associated subcategories. For instance, the standards fully address the subcategories for credentials to be issued, managed, verified, revoked, and audited for authorized devices, users, and processes; network integrity to be protected; and physical access to assets to be managed and protected.
- The standards fully address the response planning category by fully addressing the associated subcategory—a response plan is to be executed during or after an incident.

Conversely, the FERC-approved cybersecurity standards partially address or do not address the remaining 15 of 23 categories. For example:

- The standards partially address the category for supply chain risk management. In particular, the standards fully address associated subcategories for establishing supply chain risk management processes, security measures in contracts with suppliers and third-party partners, and evaluations of suppliers and third-party partners to ensure they meet their contractual obligations. However, the standards do not address subcategories for response and recovery planning and testing with suppliers and third-party providers, and for using the supply chain risk management process to identify, prioritize, and assess suppliers and third-party partners.
- The standards do not address the three subcategories associated with the risk management strategy category. Specifically, the standards do not call for risk management processes to be established, organizational risk tolerance to be determined, or for the risk tolerance to be informed by the organization's role in critical infrastructure and sector-specific risk analysis.

In a written response, FERC officials said that the agency did not conduct an assessment to determine how the leading practices identified in the NIST Cybersecurity Framework could be applied to the cybersecurity standards. In addition, FERC officials stated that, while the Commission uses the NIST Cybersecurity Framework as a resource and its approved standards incorporate certain facets of the framework, there is not a one-on-one alignment because the NIST Cybersecurity Framework is not industry specific. According to FERC officials, the framework addresses

certain issues outside FERC's jurisdiction. For example, FERC officials stated that the Commission does not have authority to directly impose obligations on suppliers, vendors, or entities outside its jurisdiction that provide products or services to electric industry stakeholders.

However, full implementation of the NIST Cybersecurity Framework does not require regulatory agencies to impose obligations on entities over which the regulatory agencies do not have authority. Framework categories and subcategories that reference suppliers and vendors call for the organization responsible for implementing the framework to establish and implement processes for managing cybersecurity risks relating to those suppliers and vendors.

In addition, in a written response, NERC officials disagreed with our assessment and stated that a separate comparison by NERC subject matter experts found substantially more overlap between the FERC-approved cybersecurity standards and the NIST Cybersecurity Framework.⁷⁷ Moreover, NERC officials said that the intended purpose of the standards differs from the framework's voluntary nature, and that NERC must ensure all mandatory standards are auditable and implemented by electric utilities nationwide. The officials noted the importance of the NIST Cybersecurity Framework and emphasized that NERC has considered the framework in developing and updating grid cybersecurity standards. However, we believe our analysis accurately reflects the extent that the FERC-approved standards address the NIST Cybersecurity Framework.

Without a full consideration of how the FERC-approved cybersecurity standards address NIST's Cybersecurity Framework, there is increased risk that bulk power entities will not fully implement leading cybersecurity practices intended to help critical infrastructure entities address cybersecurity risks.

⁷⁷NERC officials also cited a 2011 GAO report that found the standards substantially similar to certain NIST guidance. Specifically, in *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use* (GAO-12-92), we reported that, together, FERC-approved cybersecurity standards and NERC supplementary guidance mostly addressed the information security controls in NIST SP 800-53 Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations* (May 2010). In contrast, in this report we assessed the extent to which the FERC-approved cybersecurity standards addressed the more recent and broader NIST Cybersecurity Framework.

FERC Has Not Evaluated the Risk of Geographically Distributed Cyberattacks in Approving the Threshold for Required Compliance with All Cybersecurity Standards

As previously mentioned, FERC requires cyber systems affecting a generation capacity of 1,500 megawatts or more to comply with requirements in the full set of approved cybersecurity standards since the loss, compromise, or misuse of those systems could have a medium to high impact on the reliable operation of the bulk electric system.⁷⁸ FERC approved the 1,500-megawatt threshold based on the results of a NERC analysis.⁷⁹ Specifically, NERC staff selected a threshold value based on the loss of one large electric grid asset from a single disruptive event and assumed a loss of power could be compensated, in part, by power from a neighboring region.⁸⁰

However, the analysis did not evaluate the potential risk of a coordinated cyberattack on geographically distributed targets. A coordinated cyberattack could cause multiple power plants, transmission lines, or related grid components in different regions to disconnect from the grid. Such a cyberattack could target, for example, a combination of low-impact systems, each affecting a generation capacity below 1,500 megawatts that, in aggregate, might present a significant risk to the grid.

FERC officials told us that the agency considered but did not evaluate the potential impact of a coordinated cyberattack on geographically distributed targets at the time it approved the threshold because the agency did not have the information it needed to develop a credible threat

⁷⁸Specifically, FERC requires systems affecting net aggregate generation capacity of 1,500 megawatts or more at one power plant location within a single interconnection to comply with requirements in the full set of its approved cybersecurity standards. The standards contain additional criteria that allow regulated entities to designate power plants with a generation capacity of less than 1,500 megawatts as being subject to the requirements of the full set of cybersecurity standards. In particular, NERC officials told us that, in the event a system planner or reliability coordinator for given areas finds that a power plant with a generation capacity of less than 1,500 megawatts presents risks to the system and should be protected at a higher level, that entity may designate the power plant as medium-impact and therefore be subject to the full set of cybersecurity standards. However, according to FERC officials, FERC does not track or retain information on which plants are thus designated beyond the scope of an individual audit.

⁷⁹CIP-002-5.1a explains that the 1,500-megawatt threshold was “sourced partly from the contingency reserve requirements in” NERC’s BAL-002 standard, which is designed to ensure sufficient contingency reserve to cover the most severe single disruptive event. FERC staff were unable to provide other supporting analysis for the threshold.

⁸⁰NERC’s analysis was based on 66 regions across the contiguous United States, in which balancing authorities maintain the balance of generation and consumption. According to NERC officials, the analysis was informed by industry subject matter expertise and the best understanding of cyber risk at the time.

scenario. FERC officials said they anticipate that a future update to the approved cybersecurity standards may require the collection of relevant data on suspicious cyber activity that could inform a threat scenario for evaluating the potential impact of a coordinated cyberattack on geographically distributed targets.⁸¹ Further, NERC officials told us that, while NERC has not determined that a modification of the 1,500 megawatt threshold is warranted at this time, they continue to monitor the risk of a coordinated cyberattack against multiple low-impact systems and acknowledged that the FERC-approved standards must adapt with the evolving understanding of cyber threats.

In addition, NERC officials explained in a written response that the intent of the 1,500-megawatt threshold is to ensure that industrial control systems with vulnerabilities that are attributable to a common cause (e.g., cybersecurity vulnerabilities in common hardware or software) that could result in the loss of 1,500 megawatts or more of generation capacity are adequately protected. Those officials added that NERC encourages entities to disaggregate their industrial control systems so that individual systems operate and maintain less than 1,500 megawatts of generation capacity. NERC officials noted that the systems associated with the disaggregated generation capacity are very diverse and are therefore less likely to provide any large single point of failure. NERC officials further explained that this disaggregation minimizes the risk to the grid by requiring a malicious actor to conduct a cyberattack on more facilities to achieve a similar loss of power.

However, encouraging grid entities to design industrial control systems so that individual systems operate and maintain less than 1,500 megawatts of generation capacity could still leave the grid vulnerable to a cyberattack on those systems. For example, although a malicious actor may need to attack more systems that fall under the threshold at multiple locations to achieve the attacker's objective for loss of power (when compared with systems that meet or exceed the threshold), the difficulty of carrying out an attack on additional systems could be less significant if the attacker identifies and exploits vulnerabilities common across the systems. In

⁸¹FERC issued an order on June 20, 2019 approving CIP-008-6: Incident Reporting and Response Planning, which broadens mandatory reporting to include cybersecurity incidents that compromise, or attempt to compromise, a responsible entity's electronic security perimeter or associated electronic access control or monitoring systems, as well as modifications to specify the required information in cybersecurity incident reports, their dissemination, and deadlines for filing reports. The revised standard will become effective January 1, 2021.

addition, as previously mentioned, systems that fall under the 1,500-megawatt threshold are not required to follow all of the requirements of the FERC-approved cybersecurity standards; as such, there is increased risk that important security controls have not been implemented for these systems.

According to federal standards for internal control, management should identify, analyze, and respond to risks related to achieving organizational objectives.⁸² For example, management comprehensively identifies risks that affect its objectives and analyzes the identified risks to estimate their significance, which provides a basis for responding to the risks.

Without information on the risk of a coordinated cyberattack on geographically distributed targets, FERC does not have assurance that its approved threshold for mandatory compliance with all cybersecurity standards adequately responds to that risk and sufficiently provides for the reliable operation of the grid.

Conclusions

The U.S. electric grid faces an increasing array of cybersecurity risks, as well as significant challenges to addressing those risks. To their credit, federal agencies have performed a variety of critical infrastructure protection and regulatory activities aimed at addressing those risks. In particular, DOE has developed plans and an assessment aimed at implementing the federal strategy for confronting the cyber threats facing the grid. However, those documents do not fully address all of the key characteristics needed to implement a national strategy, including a full assessment of cybersecurity risks to the grid. Until DOE ensures it has a plan that does, the guidance the plan provides decision makers in allocating resources to address grid cybersecurity risks and challenges will likely be limited.

Additionally, FERC has approved mandatory cybersecurity standards for bulk power entities, but those standards address some but not all of the leading cybersecurity practices identified in NIST's Cybersecurity Framework. Without a full consideration of how the FERC-approved cybersecurity standards address NIST's Cybersecurity Framework, there

⁸²GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014).

is increased risk that bulk power entities will not fully implement leading cybersecurity practices needed to address current and projected risks.

Finally, the threshold for which entities must comply with requirements in the full set of FERC-approved standards is based on the results of an analysis that did not evaluate the potential risk of a coordinated cyberattack on geographically distributed targets. Without information on the risk of such an attack—particularly one that might target low-impact systems that are subject to fewer requirements but in aggregate could affect the grid—FERC does not have assurance that its approved threshold for mandatory compliance adequately responds to that risk and sufficiently provides for the reliable operation of the electric grid.

Recommendations for Executive Action

We are making a total of three recommendations—one to DOE and two to FERC. Specifically:

- The Secretary of Energy, in coordination with DHS and other relevant stakeholders, should develop a plan aimed at implementing the federal cybersecurity strategy for the electric grid and ensure that the plan addresses the key characteristics of a national strategy, including a full assessment of cybersecurity risks to the grid. (Recommendation 1)
- FERC should consider our assessment and determine whether to direct NERC to adopt any changes to its cybersecurity standards to ensure those standards more fully address the NIST Cybersecurity framework and address current and projected risks. (Recommendation 2)
- FERC should (1) evaluate the potential risk of a coordinated cyberattack on geographically distributed targets and, (2) based on the results of that evaluation, determine whether to direct NERC to make any changes to the threshold for mandatory compliance with requirements in the full set of cybersecurity standards. (Recommendation 3)

Agency Comments, Third-Party Views, and Our Evaluation

We provided a draft of this report for review and comment to DOE and FERC—the two agencies to which we made recommendations—as well as DHS, the Department of Commerce (on behalf of NIST), and NERC. DOE and FERC agreed with our recommendations, DHS and the Department of Commerce stated that they had no comments, and NERC disagreed with one of our findings.

DOE and FERC agreed with our recommendations. In its written comments, reproduced in appendix III, DOE concurred with our recommendation and stated that it is working through an interagency process to develop a *National Cyber Strategy Implementation Plan* that will consider DOE's *Multiyear Plan for Energy Sector Cybersecurity*. In its written comments, reproduced in appendix IV, FERC stated that our recommendations were constructive and that it would take steps to implement them. DOE and FERC also provided technical comments, which we incorporated as appropriate.

In its written comments, reproduced in appendix V, NERC stated that it disagreed with our conclusion that the FERC-approved cybersecurity standards do not fully address the NIST Cybersecurity Framework. NERC recognized the importance of the NIST Cybersecurity Framework and emphasized that NERC has considered the framework in developing and updating its grid cybersecurity standards. However, NERC stated that a separate analysis by NERC subject matter experts found substantially more overlap between the standards and the framework than our analysis. In addition, NERC cited a 2011 GAO report that found that the FERC-approved standards, in combination with NERC supplementary guidance, mostly addressed the information security controls in certain NIST guidance at that time.⁸³

We reviewed NERC's analysis comparing the FERC-approved cybersecurity standards to the NIST Cybersecurity Framework and continue to believe our analysis accurately reflects the extent to which the standards address the framework. Further, in this report we assessed the extent to which the FERC-approved standards addressed the NIST Cybersecurity Framework, which is more recent and broader guidance than the NIST guidance that we examined in our 2011 report.

In its comments, NERC also stated it has not determined that any changes are needed to the threshold for mandatory compliance with the full set of cybersecurity standards at this time, but it agrees with the concern that low-impact systems may be more vulnerable to a cyberattack and will continue to evaluate whether the current threshold is appropriate given evolving cybersecurity risks. For example, NERC explained that it is studying cybersecurity supply chain risks, including those associated with low-impact assets not currently subject to its supply

⁸³[GAO-12-92](#).

chain standards. We believe that this effort could help to better position electric grid entities to address supply chain cybersecurity risks.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the appropriate congressional committees, the Secretaries of Commerce, Energy, and Homeland Security, the Chairman of FERC, and other interested parties. In addition, the report will be available at no charge on the GAO website at <http://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 VI.



Frank Rusco
Director, Natural Resources and Environment



Nick Marinos
Director, Information Technology and Cybersecurity

List of Requesters

The Honorable Frank Pallone, Jr.
Chairman
Committee on Energy and Commerce
House of Representatives

The Honorable Bobby L. Rush
Chairman
Subcommittee on Energy
Committee on Energy and Commerce
House of Representatives

The Honorable Jerry McNerney
House of Representatives

The Honorable Paul D. Tonko
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the cybersecurity risks and challenges facing the electric grid, (2) describe federal efforts to address grid cybersecurity risks, (3) assess the extent to which the Department of Energy (DOE) has a defined strategy for addressing grid cybersecurity risks and challenges, and (4) assess the extent to which Federal Energy Regulatory Commission (FERC)-approved cybersecurity standards address grid cybersecurity risks.

To address our first objective, we developed a list of cyber actors that could pose a threat to the grid, identified vulnerable components and processes that could be exploited, reviewed the potential impact of cyberattacks on the grid, and identified key cybersecurity challenges facing the grid. To develop the list of cyber threat actors, we reviewed our prior work on cyber-based threats facing the grid¹ as well as the threats identified by the 2019 *Worldwide Threat Assessment of the U.S. Intelligence Community*.² In addition, we interviewed officials or representatives from the following key federal and nonfederal entities to confirm, add, or remove cyber threat actors identified in our prior work based on their potential impact on grid operations:

- **Federal agencies.** We interviewed officials from DOE,³ the Department of Homeland Security (DHS), FERC, and the National Institute of Standards and Technology (NIST).
- **Nonfederal regulatory organizations.** We interviewed representatives of the North American Electric Reliability Corporation (NERC).

¹GAO, *Cybersecurity: Challenges in Securing the Electric Grid*, [GAO-12-926T](#) (Washington, D.C.: July 17, 2012).

²Daniel 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.

³We interviewed officials from DOE's Office of Cybersecurity, Energy Security, and Emergency Response as well as the following national laboratories: Argonne National Laboratory, Brookhaven National Laboratory, Fermi National Accelerator Laboratory, Idaho National Laboratory, Lawrence Berkeley National Laboratory, Lawrence Livermore National Laboratory, Los Alamos National Laboratory, National Energy Technology Laboratory, National Renewable Energy Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, Princeton Plasma Physics Laboratory, Sandia National Laboratories, Savannah River National Laboratory, Stanford Linear Accelerator Center National Accelerator Laboratory, and Thomas Jefferson National Accelerator Facility.

- **Grid owners and operators.** We interviewed five grid owners and operators. To select these grid owners and operators, we reviewed a membership list of the Electricity Subsector Coordinating Council as of May 2018, divided that list into three categories—investor-owned, municipal, and cooperative utilities—and then randomly selected entities from each of those three categories to interview. The views of the grid owners and operators we selected are not generalizable to the population of utilities in the United States but provide valuable insight into the cybersecurity risks and challenges grid owners and operators face.
- **National associations.** We interviewed representatives of national associations that represent various types of asset owners, entities with regulatory or state interests, and those with grid cybersecurity interests generally. Specifically, we interviewed representatives from the American Public Power Association, Edison Electric Institute, Electric Power Research Institute, Independent System Operator/Regional Transmission Operator Coordinating Council, National Rural Electric Cooperative Association, National Association of Regulatory Utility Commissioners, National Association of State Energy Officials, and North American Transmission Forum Association. The views of the association representatives are not generalizable to the industry but provide valuable insight into the cybersecurity risks and challenges facing the grid.

To identify grid cybersecurity vulnerabilities, we reviewed reports developed by key federal and nonfederal entities and others related to grid vulnerabilities⁴ and met with the key federal and nonfederal entities to understand the scale and complexity of these vulnerabilities. We also compiled DHS-provided advisories from 2010 through 2018 related to industrial control system devices. We then summarized information from the DHS website to determine how many DHS issued per year.

With respect to the potential impact of cyberattacks, we reviewed cybersecurity incidents reported to DOE, DHS, and NERC from 2014 through 2018. We also asked these agencies for information on any cybersecurity incidents that occurred prior to 2014 or after 2018 that

⁴E.g., Department of Energy, Infrastructure Security and Energy Restoration, *Electricity Subsector Risk Characterization Study* (2017-2019); Department of Energy, Idaho National Laboratory, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector: Mission Support Center Analysis Report* (August 2016); and S. Soltan, P. Mittal, and H.V. Poor, "BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid," 27th USENIX Security Symposium, Baltimore, MD, August 15–17, 2018.

affected the reliability or availability of the grid. In addition, we reviewed federal reports on cyberattacks that caused power outages in foreign countries⁵ and a report developed by the German government regarding a cyberattack on industrial control systems that damaged a German steel mill.⁶ Further, we reviewed federal studies assessing the potential for widespread power outages resulting from cyberattacks,⁷ and we met with federal officials to discuss the methodologies used to perform these studies. Finally, to identify key cybersecurity challenges facing the grid, we reviewed our prior reports on such challenges⁸ as well as federal and industry reports recommended by entities we met with.⁹ We also asked the key federal and nonfederal entities to identify challenges facing grid entities in addressing cybersecurity risks, and we compiled the challenges they most often cited.

To address the second objective, we identified critical infrastructure protection and regulatory actions that federal agencies are taking to address grid cybersecurity risks by reviewing federal strategies, plans, and reports describing activities that have been conducted or that are under way and by interviewing the key federal and nonfederal entities to obtain additional details on these activities. We also reviewed FERC-

⁵See, e.g., Department of Homeland Security, *Cyber-Attack against Ukrainian Critical Infrastructure Alert*, IR-ALERT-H-16-056-01 (February 25, 2016).

⁶German Federal Office for Information Security, "Incidents in the Economy," *The State of IT Security in Germany* (2014).

⁷Federal Energy Regulatory Commission, *OEIS/OER Response to Questions Identifying Electrically Significant Locations on the Bulk Power System* (2013); Department of Energy, Infrastructure Security and Energy Restoration, *Electricity Subsector Risk Characterization Study* (2017, 2018, 2019); and Department of Energy, Argonne National Laboratory, *Analysis of Electricity Transfer Capabilities Among Region V Regional Transmission Organizations* (2017).

⁸GAO, *Electricity: Federal Efforts to Enhance Grid Resilience*, [GAO-17-153](#) (Washington, D.C.: Jan. 25, 2017); *Cybersecurity: Challenges in Securing the Modernized Electricity Grid*, [GAO-12-507T](#) (Washington, D.C.: Feb. 28, 2012); and [GAO-12-926T](#).

⁹E.g., North American Electric Reliability Corporation, *Grid Security Exercise GridEx IV: Lessons Learned* (March 2018); Department of Energy, Idaho National Laboratory, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector: Mission Support Center Analysis Report* (August 2016).

approved cybersecurity standards for the bulk power system.¹⁰ We then categorized critical infrastructure protection activities using the functions in NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (commonly referred to as NIST's Cybersecurity Framework).¹¹

For our third objective, we reviewed two DOE-led plans and one assessment aimed at implementing the federal cybersecurity strategy for the energy sector, including the grid.¹² We then compared those plans and assessment with leading practices identified by GAO on key characteristics for a national strategy.¹³ In doing so, we assessed each characteristic as follows:

- **fully addresses**—the plan or assessment addresses all aspects of the characteristic,
- **partially addresses**—the plan or assessment addresses some but not all of the characteristic, or
- **does not address**—the plan or assessment does not address any aspects of the characteristic.

We also provided our analysis to DOE officials to review, comment, and provide additional information.

For our fourth objective, we compared the FERC-approved cybersecurity standards with leading federal practices for addressing critical infrastructure cybersecurity risks identified in NIST's Cybersecurity Framework.¹⁴ Specifically, a GAO analyst compared the FERC-approved

¹⁰NERC develops reliability standards collaboratively through a deliberative process involving utilities and others in the industry, which are then sent to FERC for approval. These standards include critical infrastructure protection standards for protecting electric utility-critical and cyber-critical assets. FERC reviews reliability standards and may approve them or remand them to NERC for revision.

¹¹National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (Gaithersburg, MD.: April 2018).

¹²Department of Energy and Department of Homeland Security, *Energy Sector-Specific Plan, 2015* (Washington, D.C.: 2015); Department of Energy and Department of Homeland Security, *Assessment Of Electricity Disruption Incident Response Capabilities* (Washington, D.C.: May 2018); Department of Energy, *Multiyear Plan for Energy Sector Cybersecurity* (Washington, D.C.: May 2018).

¹³GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

¹⁴National Institute of Standards and Technology, *Cybersecurity Framework*.

cybersecurity standards with the subcategories in the Cybersecurity Framework, and another GAO analyst reviewed and confirmed the results of that analysis.¹⁵ We then summarized the results of these assessments for each of the framework's five functions, 23 categories, and 108 subcategories as follows:

- **fully address**—the standards address all of the related subcategories;
- **substantially address**—the standards address at least two-thirds, but not all, of the related subcategories;
- **partially address**—the standards address at least one-third, but less than two-thirds, of the related subcategories;
- **minimally address**—the standards address less than one-third of the related subcategories; or
- **do not address**—the standards do not address any of the related subcategories.

We also provided our analysis to FERC and NERC officials to review, comment, and provide additional information.

We also examined the applicability of the FERC-approved cybersecurity standards to non-nuclear power plants and reviewed FERC and NERC information on the analytical basis for that threshold.¹⁶ To calculate the number and aggregate capacity of plants that met the 1,500-megawatt threshold for complying with all FERC-approved cybersecurity standards, we used data from Form EIA-860, "Annual Electric Generator Report," which includes U.S. plants with generators having nameplate capacity¹⁷

¹⁵Four of the cybersecurity standards we included in this analysis have been approved by FERC but are subject to future enforcement. Three of those standards are updates to existing standards: CIP-003-7 Security Management Controls, CIP-005-6 – Electronic Security Perimeter(s), and CIP-010-3 Configuration Change Management and Vulnerability Assessments. The remaining standard—CIP-013-1 Supply Chain Risk Management—is a new standard. We did not consider CIP-008-6 in this analysis because it was not approved when we completed the analysis. At that time, CIP-008-5 was in effect and thus, included in the analysis.

¹⁶We excluded nuclear power plants because they are regulated by the U.S. Nuclear Regulatory Commission and are generally exempt from FERC-approved cybersecurity standards.

¹⁷According to the U.S. Energy Information Administration (EIA), nameplate capacity refers to the maximum rated output of a generator, prime mover, or other electric power production equipment under specific conditions designated by the manufacturer.

of 1 megawatt or greater. As a proxy for the net real power capability specified in the standards, we selected the generator's net summer generating capacity. To calculate a total capacity for each individual power plant, we combined the data on the capacity of each plant's individual operating electric power generators. We then filtered these data to identify plants whose primary purpose is generating electricity for sale as reported on the Form EIA-860. Ultimately, we compared the number and capacity of non-nuclear plants exceeding the 1,500-megawatt threshold to the total number and total U.S. capacity for plants.

We used U.S. Energy Information Administration (EIA) data to estimate the number and capacity of non-nuclear plants exceeding the 1,500-megawatt threshold. To assess the reliability of these data, we reviewed EIA documentation, discussed the quality of the data with EIA officials, and electronically tested the data set for missing data, outliers, or obvious errors. Based on this assessment, we determined that the EIA data were sufficiently reliable for our purposes.

We conducted this performance audit from January 2018 to August 2019 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.

Appendix II: Assessment of the Extent FERC-Approved Cybersecurity Standards Address the NIST Cybersecurity Framework

The table below provides additional detail on our assessment of the extent to which Federal Energy Regulatory Commission (FERC)-approved cybersecurity standards address the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity's* (commonly known as the NIST Cybersecurity Framework) 23 categories and 108 subcategories.

Table 6: Extent to Which Federal Energy Regulatory Commission-Approved Cybersecurity Standards for Medium- and High-Impact Systems Address NIST Cybersecurity Framework Categories and Subcategories

Core function category	GAO assessment	Subcategory	GAO assessment
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business organizational objectives and the organization's risk strategy.	●	ID.AM-1: Physical devices and systems within the organization are inventoried.	○
		ID.AM-2: Software platforms and applications within the organization are inventoried.	○
		ID.AM-3: Organizational communication and data flows are mapped.	●
		ID.AM-4: External information systems are catalogued.	○
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	●
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, and partners) are established.	●
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	○	ID.BE-1: The organization's role in the supply chain is identified and communicated.	○
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated.	○
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.	○
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	○
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).	○
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood	●	ID.GV-1: Organizational information security cybersecurity policy is established and communicated.	●
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	○

Appendix II: Assessment of the Extent FERC-Approved Cybersecurity Standards Address the NIST Cybersecurity Framework

Core function category	GAO assessment	Subcategory	GAO assessment
and inform the management of cybersecurity risk.		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	○
		ID.GV-4: Governance and risk management processes address cybersecurity risks.	●
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	●	ID.RA-1: Asset vulnerabilities are identified and documented.	●
		ID.RA-2: Cyber threat intelligence is received from information-sharing forums and sources.	○
		ID.RA-3: Threats, both internal and external, are identified and documented.	●
		ID.RA-4: Potential business impacts and likelihoods are identified.	●
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	●
		ID.RA-6: Risk responses are identified and prioritized.	●
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	○	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	○
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed.	○
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	○
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.	●	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	●
		ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	○
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	●
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	●
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	○

Appendix II: Assessment of the Extent FERC-Approved Cybersecurity Standards Address the NIST Cybersecurity Framework

Core function category	GAO assessment	Subcategory	GAO assessment
Identity Management Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	●	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	●
		PR.AC-2: Physical access to assets is managed and protected.	●
		PR.AC-3: Remote access is managed.	●
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	●
		PR.AC-5: Network integrity is protected (e.g. network segregation and network segmentation).	●
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	●
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	●
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related cybersecurity duties and responsibilities consistent with related policies, procedures, and agreements.	①	PR.AT-1: All users are informed and trained.	●
		PR.AT-2: Privileged users understand their roles and responsibilities.	○
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, and partners) understand their roles and responsibilities.	●
		PR.AT-4: Senior executives understand their roles and responsibilities.	○
		PR.AT-5: Physical and information security cybersecurity personnel understand their roles and responsibilities.	●
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	①	PR.DS-1: Data-at-rest is protected.	●
		PR.DS-2: Data-in-transit is protected.	●
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	●
		PR.DS-4: Adequate capacity to ensure availability is maintained.	○
		PR.DS-5: Protections against data leaks are implemented.	●
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	●
		PR.DS-7: The development and testing environment(s) are separate from the production environment.	○
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	○

Appendix II: Assessment of the Extent FERC-Approved Cybersecurity Standards Address the NIST Cybersecurity Framework

Core function category	GAO assessment	Subcategory	GAO assessment
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	●	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).	●
		PR.IP-2: A System Development Life Cycle to manage systems is implemented.	○
		PR.IP-3: Configuration change control processes are in place.	●
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically.	●
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	○
		PR.IP-6: Data are destroyed according to policy.	●
		PR.IP-7: Protection processes are continuously improved.	○
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties.	○
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	●
		PR.IP-10: Response and recovery plans are tested.	●
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning and personnel screening).	●
		PR.IP-12: A vulnerability management plan is developed and implemented.	●
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	●	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	●
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	○
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	●	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	●
		PR.PT-2: Removable media is protected and its use restricted according to policy.	●
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	○
		PR.PT-4: Communications and control networks are protected.	●

Appendix II: Assessment of the Extent FERC-Approved Cybersecurity Standards Address the NIST Cybersecurity Framework

Core function category	GAO assessment	Subcategory	GAO assessment
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	○
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	●	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	○
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	○
		DE.AE-3: Event data are aggregated, collected, and correlated from multiple sources and sensors.	○
		DE.AE-4: Impact of events is determined.	●
		DE.AE-5: Incident alert thresholds are established.	●
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	●	DE.CM-1: The network is monitored to detect potential cybersecurity events.	●
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	●
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	●
		DE.CM-4: Malicious code is detected.	●
		DE.CM-5: Unauthorized mobile code is detected.	○
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	○
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	○
		DE.CM-8: Vulnerability scans are performed.	●
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	●	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.	●
		DE.DP-2: Detection activities comply with all applicable requirements.	○
		DE.DP-3: Detection processes are tested.	○
		DE.DP-4: Event detection information is communicated to appropriate parties.	●
		DE.DP-5: Detection processes are continuously improved.	○
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity events.	●	RS.RP-1: Response plan is executed during or after an event.	●
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g., as appropriate, to include external support	●	RS.CO-1: Personnel know their roles and order of operations when a response is needed.	●
		RS.CO-2: Incidents are reported consistent with established criteria.	●

Appendix II: Assessment of the Extent FERC-Approved Cybersecurity Standards Address the NIST Cybersecurity Framework

Core function category	GAO assessment	Subcategory	GAO assessment
from law enforcement agencies).		RS.CO-3: Information is shared consistent with response plans.	●
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	●
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	●
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	●	RS.AN-1: Notifications from detection systems are investigated.	●
		RS.AN-2: The impact of the incident is understood.	○
		RS.AN-3: Forensics are performed.	●
		RS.AN-4: Incidents are categorized consistent with response plans.	●
		RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).	○
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	●	RS.MI-1: Incidents are contained.	○
		RS.MI-2: Incidents are mitigated.	○
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	●
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	●	RS.IM-1: Response plans incorporate lessons learned.	●
		RS.IM-2: Response strategies are updated.	●
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	●	RC.RP-1: Recovery plan is executed during or after a cybersecurity event.	●
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	●	RC.IM-1: Recovery plans incorporate lessons learned.	●
		RC.IM-2: Recovery strategies are updated.	●
Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other Computer Security Incident Response Teams, and vendors).	○	RC.CO-1: Public relations are managed.	○
		RC.CO-2: Reputation after an event is repaired.	○
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as to executive and management teams.	○

Legend: ●—Fully address: the standards address all of the related subcategories. ●—Substantially address: the standards address at least two-thirds, but not all, of the related subcategories. ●—Partially address: the standards address at least one-third, but less than two-thirds, of the related

**Appendix II: Assessment of the Extent FERC-
Approved Cybersecurity Standards Address
the NIST Cybersecurity Framework**

subcategories. ○—Minimally address: the standards address less than one-third of the related subcategories. ○—Do not address: the standards do not address any of the related subcategories.

Source: GAO analysis of North American Electricity Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards in comparison with functions and categories in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. | GAO-19-332

Appendix III: Comments from the Department of Energy

The report number GAO-19-332SU has been changed to GAO-19-332.



Department of Energy
Washington, DC 20585

August 2, 2019

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

Dear Mr. Rusco:

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, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid, GAO-19-332SU*. As the Sector-Specific Agency (SSA) for energy sector cybersecurity, DOE takes this responsibility seriously, particularly in the face of increasing cyber risk to critical energy sector assets, nodes, and functions.

Cybersecurity risks are constantly evolving. DOE is working to put processes and procedures in place to: 1) understand the ever-changing threats and hazards; 2) understand the grid's cybersecurity vulnerabilities; 3) understand the potential magnitude of impacts and consequences; and, 4) identify and facilitate implementation of mitigation strategies. DOE plans to keep the Department's efforts ongoing for the four key elements mentioned above.

The draft report contained a total of three recommendations, of which GAO directed one recommendation to DOE. DOE concurs with GAO's recommendation. Details regarding GAO's recommendation, and DOE's technical comments on the draft report are provided enclosure. In addition to the technical comments enclosed, extensive technical comments and security concerns were provided through my office via a conference call with GAO staff on July 29.

GAO should direct any questions to Adrienne Lotto, Deputy Assistant Secretary for Infrastructure Security and Energy Restoration, at adrienne.lotto@hq.doe.gov or 202-586-1117.

Sincerely,

A handwritten signature in black ink, appearing to read "Karen S. Evans".

Karen S. Evans
Assistant Secretary
Office of Cybersecurity, Energy Security, and
Emergency Response

Enclosure



ENCLOSURE

Response to Report Recommendation

Recommendation 1: *The Secretary of Energy, in coordination with DHS and other relevant stakeholders, should develop a plan aimed at implementing the federal cybersecurity strategy for the electric grid and ensure that the plan addresses the key characteristics of a national strategy, including a full assessment of cybersecurity risks to the grid.*

Management Response: Concur.

The Office of Cybersecurity, Energy Security, and Emergency Response (CESER) agrees with the principles outlined in the draft report. DOE's current actions meet the intent of GAO's recommendation.

DOE has been working through the National Security Council (NSC) to develop a National Cyber Strategy Implementation Plan, in an interagency process whereby agencies identified in National Security Presidential Memorandum (NSPM-4) collaborate to develop activities that need to be jointly worked on and sector-specific activities. The NSC Implementation Plan takes into consideration DOE's Multiyear Plan for Energy Sector Cybersecurity. The Implementation Plan is expected to be completed in fall 2019.

DOE actively works with Department of Homeland Security's (DHS) National Risk Management Center (NRMCC) on the identification of national critical functions¹ — to prioritize sector-specific and cross-sector activities. DOE will continue to work with the energy sector through the Sector Coordinating Councils (SCC), the Electricity Subsector Coordinating Council (ESCC) and Oil and Natural Gas Subsector Coordinating Council (ONG SCC), in addressing cybersecurity risks to the sector.

Estimated Completion Date: December 31, 2019.

¹ <https://www.dhs.gov/cisa/national-critical-functions-set>

Appendix IV: Comments from the Federal Energy Regulatory Commission

The report number GAO-19-332SU has been changed to GAO-19-332.

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

July 15, 2019

Frank Rusco
Director, Natural Resources and Environment

Nick Marinos
Director, Information Technology and Cybersecurity

Government Accountability Office
441 G St., NW
Washington, DC 20548

Subject: GAO-19-332SU – Critical Energy Infrastructure– Draft Report

Dear Mr. Rusco and Mr. Marinos:

Thank you for the opportunity to provide comments on behalf of the Federal Energy Regulatory Commission (Commission) with respect to the Government Accountability Office's (GAO) draft report entitled, "Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid."

The Commission recognizes that cyber-attacks on our critical infrastructure systems have the potential to create significant, widespread, and potentially devastating effects that threaten the health, safety, and economic prosperity of the American people whom we serve. With this recognition, the Commission has and continues to address cybersecurity risks as consistent with section 215 of the Federal Power Act, which grants us the authority to approve and enforce mandatory Reliability Standards developed by the North American Electric Reliability Corporation (NERC). The Commission also has taken up voluntary initiatives with federal, state, and industry partners to address cybersecurity issues for critical energy infrastructure, including efforts to identify and share best practices. The responsibility for securing critical infrastructure is shared by industry and government authorities at the federal and state levels, and it is imperative that we continue to strengthen these partnerships.

GAO's draft report also recognizes the importance of these cybersecurity issues and is a timely contribution on the subject. In the draft report, GAO makes the following recommendations with regard to the Commission:

GAO-19-332SU – Critical Energy Infrastructure– Draft Report

- Consider adopting changes to its approved cybersecurity standards to more fully address the NIST Cybersecurity Framework. (Recommendation 2); and
- Evaluate the potential risk of a coordinated cyber-attack on geographically distributed targets, and based on the results of that evaluation, determine if changes are needed in the threshold for mandatory compliance with requirements in the full set of cybersecurity standards. (Recommendation 3)

I believe that these recommendations are constructive, and I have directed Commission staff to develop appropriate next steps to implement them.

I greatly appreciate the courtesies extended to FERC staff throughout GAO's development of the draft report.

Sincerely,



Neil Chatterjee
Chairman

Appendix V: Comments from the North American Electric Reliability Corporation

The report number GAO-19-332SU has been changed to GAO-19-332.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

James B. Robb
President and Chief Executive Officer

July 26, 2019

Mr. Frank Rusco
Director, Natural Resources and Environment

Mr. Nick Marinos
Director, Information Technology and Cybersecurity

Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Rusco and Mr. Marinos:

NERC appreciates the opportunity to provide technical input to the U.S. Government Accountability Office (GAO) for the draft report, "Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid" (Report). NERC believes this is an important assessment and we appreciate the numerous meetings we have had with GAO staff on this engagement. There are two areas where we think the draft report does not adequately reflect our input. For those two findings and recommendations, we would like to provide the following perspective.

NIST Cybersecurity Framework: With respect to the NIST framework, Table 5 includes GAO's assessment of the extent to which NERC critical infrastructure protection standards (CIP or CIP standards) address the NIST framework, finding that NERC's CIP standards only partially address the practices covered in the NIST framework and in some cases not at all. NERC disagrees with GAO's conclusion. We believe the Report should recognize that NERC strongly considered the NIST framework during development of the CIP standards and continues to consider the framework in further updates and improvements. While the framework is a widely recognized model, it is important to note that the intended purpose of NERC's mandatory standards differs from the NIST framework's voluntary nature. The voluntary nature of the NIST framework allows entities to customize protections for their particular needs depending on specific situations. NERC must ensure that each mandatory standard requirement is auditable and consistently implemented by electric organizations across the continent.

NERC recognizes the importance of the NIST Cybersecurity Framework and works to ensure all elements of the NIST framework's voluntary efforts are taken into consideration and tracked to all mandatory CIP standards. A separate comparison by a team of NERC subject matter experts – which we provided to GAO – has found substantially more overlap with CIP than GAO found. To fully inform readers, NERC believes the NERC comparison should be included in the final report.

In an earlier report conducted by GAO in 2011, GAO requested similar information from NERC, asking for a comparison of NERC standards to, at that time, the NIST risk management framework. In that report, GAO included the information and acknowledged that NERC cyber security standards addressed the NIST risk management framework, even noting NERC's concern with comparing the two. NERC strongly considered the NIST framework

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

RELIABILITY | ACCOUNTABILITY



during development of the CIP standards and continues to consider the framework in working to update and improve those standards.¹ We believe the Report should acknowledge this work.

Threshold for generation units: The CIP standards are based on the premise that the level of mandatory protections applied to a particular cyber system should be commensurate to the system's potential impact on the bulk power system if the cyber system was lost, compromised, or misused. To that end, Reliability Standard CIP-002-5.1a requires entities to identify BES Cyber Systems and categorize them as low-, medium-, or high-impact systems based upon the adverse impact that loss, compromise, or misuse of those systems could have on bulk power system reliability. This approach ensures efficient and effective allocation of resources protecting critical infrastructure, thus providing regulatory certainty and maximizing overall benefits to reliability.

It is important to note that the electric system is designed with a high level of networking and redundancy and, by design, focuses on minimizing "too big to fail" assets. Based on an analysis by industry subject matter experts, cyber systems associated with groupings of generation units below 1,500 megawatts have a low impact rating. This "bright-line criteria" encourages power producers to segment groupings of generating units below the threshold in order to minimize risk. Entities with these low impact systems are required to implement risk-informed policies addressing electronic access controls, physical security controls, cyber security awareness, and cyber security incident response (Reliability Standard CIP-003-6). Further, in the event a system planner or a reliability coordinator for a given area finds that a generation unit below 1,500 MW presents risks to the system and should be protected at a higher level, the CIP standards allow (or require) that entity to designate that generating unit as medium-impact such that the entity owning/operating that unit must comply with additional requirements.

GAO expresses concern that low impact systems may be more vulnerable to cyber attack, and that reclassification of those systems into a higher risk category could provide greater protection against a coordinated attack on numerous generators across a widespread area.

It is important to stress that the existing bright-line criteria was based on industry subject matter expertise and informed by the best understanding of cyber risk at the time they were developed. That said, we agree with this concern. These currently effective bright lines have been in effect for approximately three years and, over that time, NERC has been gathering data on the effect of these thresholds on grid security. As with all of its standards, NERC continues to evaluate both (1) the level of protections required for low-impact cyber systems, and (2) the appropriateness of the existing thresholds for low-, medium-, and high-impact cyber systems. The threat of a coordinated attack against multiple low-impact cyber systems is a risk that NERC continues to monitor as it evaluates its CIP standards. We are in the process of evaluating whether the current bright line is appropriate given evolving risks to the system.

NERC recognizes that reliability standards must also adapt with our evolving understanding of cyber threats. While NERC has not determined that a modification of the bright-line criteria is warranted at this time, NERC is undertaking a similar analysis of low-impact systems in the context of the supply chain risk standards. We are gathering data and studying the nature and complexity of cyber security supply chain risks, including those associated with low-impact assets not currently subject to the supply chain standards. Similar to the evaluation recommended by GAO, NERC will employ the supply chain study to develop recommendations for follow-up actions

¹ See "CIPC Control Systems Security Working Group Mapping of NIST Cybersecurity Framework to NERC CIP v3/v5," November 2014: https://www.nerc.com/comm/CIPC_Security_Guidelines_DL/CSSWG-Mapping_of_NIST_Cybersecurity_Framework_to_NERC_CIP.pdf



that will best address identified risks. The particulars of this study are outlined in a report presented to NERC's Board of Trustees (Board) in May 2019.² We believe GAO's Report should acknowledge this effort.

Critical infrastructure protection standards are a foundation for essential cyber security practices. The electric sector is the only sector with mandatory and enforceable security standards. It is important for policymakers to understand that reliability and security depend upon many non-regulatory programs as a complement to standards.

The electric sector practices defense-in-depth and has many other programs/efforts to bolster the security posture of the industry. Executive leadership across the sector is highly committed to security, as evidenced by the very well-functioning Electricity Subsector Coordinating Council (ESCC). The ESCC is the principal liaison between leadership in the federal government and in the electric power sector, with the mission of coordinating efforts to prepare for national-level incidents or threats to critical infrastructure. The ESCC is led by CEOs from across the industry, fostering increasingly strong relationships with our government partners, including the U.S. Department of Energy (DOE), our sector specific agency.

As a member of the ESCC Steering Committee, NERC plays a leadership role in supporting ESCC initiatives. For example, the ESCC promotes robust industry support for growing the capabilities of the Electricity Information Sharing and Analysis Center (E-ISAC), which is operated by NERC as a service to industry. The E-ISAC is the central hub for the sharing of timely, actionable information on security matters. The E-ISAC has partnerships with DOE such as the Cybersecurity Risk Information Sharing Program (CRISP). CRISP is an advanced tool leveraging capabilities of DOE's National Laboratory System for sharing unclassified and classified threat information and developing mitigations to uncovered threats.

Due to the constantly evolving nature of cyber threats, E-ISAC programs are especially important in the security arena where partnerships, exercises, and information exchange are essential elements. In addition to CRISP, we conduct the biennial GridEx program and an annual week-long education and outreach program called GridSecCon, one of the largest grid security conferences available to security professionals. GridEx is consistently the largest geographically distributed grid security exercise. GridEx IV in 2017 included 6,500 individuals and 450 organizations participating across industry, law enforcement, and government agencies. This program provides entities with the means to practice their emergency response plans against the type of geographically distributed attack contemplated by GAO's recommendation. It has also led to the development of important industry initiatives such as the development of a cyber mutual assistance program.

In conclusion, we appreciate the opportunity to illuminate our concerns for GAO's recommendations, which we believe should be acknowledged in the Report along with other critical efforts the electricity sector has undertaken to strengthen its defenses and its ability to respond to a cyber attack. Thank you for your interest in NERC's mission.

Sincerely,

James B. Robb
President and Chief Executive Officer

² See NERC report, "Cyber Security Supply Chain Risks: Staff Report and Recommended Action," May 17, 2019.

Appendix VI: 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 contact named above, Kaelin Kuhn (Assistant Director), David Marroni (Assistant Director), Andrew Moore (Analyst in Charge), Dino Papanastasiou (Analyst in Charge), David Aja, Christopher Businsky, Kendall Childers, Travis Conley, Rebecca Eyler, Philip Farah, Jonathan Felbinger, Quindi Franco, Wil Gerard, Cindy Gilbert, Mike Gilmore, Andrew Howard, Paul Kazemersky, Lisa Maine, Carlo Mozo, Cynthia Norris, Sukhjoot Singh, Adam Vodraska, and Jarrod West made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<https://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <https://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707, U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.

Exhibit C
To May 11, 2020 Complaint
Submitted by Michael Mabee

Appendix II - Critical Infrastructure Protection (CIP) Standards

Limitations

In addition to structural weaknesses,¹ CIP Standards contain exclusions and specific metrics that further limit their coverage:



1. CIP Standards apply only to individual BES utilities and selected other “Registered Entities”, e.g., “balancing authorities”. Some supernumerary functionaries have “reliability authorities” but do not bring cyber assets exclusive to the function.
2. Cyber assets covered by CIP must satisfy a 15 minute “BES” impact rule to be categorized as BES Cyber Assets.
3. Metrics and other rules exclude an extensive set of generation and transmission facilities. The degree of coverage is a critical CIP issue; yet other than a slip-up during CIP v4 negotiations, NERC and FERC carefully hide these numbers from the public.²
4. Categorization of Cyber Assets excludes all communications systems and networks, one of four major exclusions from CIP 002-5. Internet connectivity is a major Grid vulnerability; it is also a significant factor in Supply Chain vulnerabilities.
5. With end-to-end modernization, operational technologies (OT) and information technologies (IT) in both Transmission and Distribution Systems are exploding, most with neither security protection nor overriding CIP Standards to ensure protection.
6. CIP Standards prevent utilities from holding their vendors responsible for penetration of the vendors’ product Supply Chain, the major attack vector for sophisticated cyber adversaries.
7. CIP Standards do not specifically address “data flows”, “data formats”, “communications protocols”, “encryption”, “data aggregations”, “analytic processes”, “control algorithms” and a myriad of other generic application areas critical to protection of the BES. (NERC will always claim that interpretive decomposition of CIP Standards suffices, making obscurity the major challenge for compliance reviewers.)
8. CIP Standards do not, as yet, require utilities to remove **known malware** from their systems.

CIP Coverage.

In negotiations on CIP v4, FERC asked for information on assets coverage for Reliability Regions. Data sent

¹ For any in-depth examination of the limitations of CIP Standards, a good starting point is the NERC report on “Remote Access required by FERC Order No. 822: Remote Access Study Report, Docket No. RM15-14-___” June 30, 2017. While NERC concludes that CIP Standards are effective in Risk Management, a good “RED TEAM” examination of this study would conclude just the opposite, flaws and huge omissions by boundary conditions put on the study would demonstrate the futility of extremely weak BES Standards protecting just the BES, let alone Distribution Utilities and Nuclear sites totally dependent on the BES for power.

² See table and comments in CIP Coverage. FERC has been challenged in several filings to task NERC for current statistics on assets within or outside CIP Standards but to no avail. Nonetheless, the display from CIP v4 development is believed to reflect current coverage in CIP v5/v6/v7.

publicly by NERC is summarized in the following table. CIP v4 was never implemented; however, nothing in follow-on CIP v5 developments would substantially change these facts; viz, substantial inconsistencies across utilities, extremely high percentage of assets exempt from coverage.

Transmission Substations Under CIP v4

Region	# Transmission Substations	# Transmission Substations ≥ 300 KV	Substations Under CIP-002-4-1.7	
			#	%
FRCC	537	16	6	37.5
MRO	1593	151	60	39.7
NPCC	809	119	39	32.8
RFC	3005	374	160	42.8
SERC	4467	283	110	38.9
SPP	1523	86	34	39.5
TRE	1182	100	50	50
WECC	3296	245	91	37.1
Totals	16412	1374	550	40.00%

We can see that only 1374 of a total of 16,412 BES Transmission Substations qualified for CIP Standards based on Kv power minimums (over 90% excluded) and of the qualifiers, only 550 (40%) were estimated by their utilities to be critical to BES Reliability. These judgments were validated by their Reliability Region, i.e., the Compliance Authority and by NERC. NERC will protest that this display does not reflect CIP v5 coverage, but rest assured, they will not voluntarily provide the current coverage statistics.

Critical Infrastructure Protection Standards

<i>CIP</i>	<i>Title</i>	<i>Definition</i>
002-5.1a	BES Cyber System Categorization	Low, Medium, High
003-5	Security Management Controls	Cybersecurity policies
004-5	Personnel and Training	Security awareness, risk assessment, access management
005-5	Electronic Security Perimeter(s)	Discrete Electronic Access Points
006-5	Physical Security BES Cyber Sys.	Physical security plan
007-5	Systems Security Management	Technical, operational and procedural steps
008-5	Incident Reporting, Response	Incident reporting -1 hour of recognition
009-5	Recovery Plans BES Cyber System	Response for stability, operability, reliability
010-1	Configuration Change Management	Monitoring, vulnerability assessment
011-1	Information Protection	Consolidation of information protection
014-1	Physical Protection	Security of Enterprise Security Perimeters

CIP Standards as they exist today are summarized in the above table. They are a subset of Reliability Standards, a much larger and more technical aggregation that were developed by the industry over the last 40 years and are kept current with the major changes in the field.³ Further, CIP Standards invoke a number of metrics from Reliability Standards and are often linked to the latter in the referenced publication. NERC Standards Development Teams (SDTs) are responsible for development. A typical CIP Standard construct consists of a purpose, applicable “Responsible Entities”, requirements that must be satisfied for CIP Cyber Systems to be covered, Violation Risk Factors, Violation Severity Levels (VSLs) to be evaluated for non-compliance, and frequently amplifying narrative. The key CIP Standard is CIP-002.5.1a since it governs categorization of BES Cyber Systems and therefore the applicability of all follow-on CIP Standards to systems so categorized.

CIP-002-5.1a

This “gateway” standard’s purpose is to identify and categorize BES Cyber Systems and their associated BES Cyber Assets. Responsible functional entities include Balancing Authorities, certain Distribution Authorities based on BES linkages, Generation Operators, Generation Owners, Interchange Authorities, Reliability Coordinator, Transmission Operator, Transmission Owner. Also defined are Facilities (types) under these authorities and BES Cyber Systems, Cyber Assets covered by Cyber Systems and Control and Monitoring and methodology permitting the flexibility the Utility has in its groupings of Cyber Assets (individually or within a Cyber System).

Attachment 1 to this CIP provides the criteria for judging whether a Cyber System (and its associated Cyber Assets) is categorized as Low, Medium or High Impact. Highlighted assets covered by that criteria are Electronic Access Control and Monitoring Systems (EACMS), Physical Access Control Systems (PACs), and Protected Cyber Assets (PCAs). ***(These Assets are the subject of a major disagreement between the Industry, NERC, and FERC over FERC’s insistence that they be included in CIP modifications for Supply Chain vulnerabilities⁴.)***

Requirement R1 details the assets to be reviewed by the “Responsible Entity” and identified as a medium or high impact asset IAW the criterial in Attachment 1. It further states: ***“Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).”***

Requirement R2 calls for a critical review of the set identifications of R1, at least every 15 months and approval of a CIP Senior manager of such decisions.

Note: The following are exclusions from CIP Cyber System Categorization:

“4.2.3. Exemptions: The following are exempt from Standard CIP-002-5.1a:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

³ NERC Reliability Standards for the Bulk Electric Systems of North America, Updated January 3, 2018

⁴ Docket No. RM17-13-000 COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.⁵

Violation Severity Levels (VSLs)

This standard includes VSLs for each of the Requirements, specified as Lower, Moderate, High or Severe. Each details the omissions or flaws revealed by the compliance audit. Penalties, if any, are not shown; left to the judgment of the CEA presumably. Note that these CIP Standards all relate to the Impact on the BES and over time, FERC has agreed to local determination by the compliance auditor, overseen by Regional Entities and ultimately by NERC. The Reliability Assessment Initiative⁶ has significantly altered the CIP Standards effectiveness in the process.

Compliance

The Regional Entity serves as the Compliance Enforcement Authority (CEA) nominally the Regional Reliability authority or his agent. Compliance evidence is retained by the CEA a minimum of 3 years unless a longer period is specified by the CEA. The Compliance Monitoring and Assessment Processes can involve any or all of the following: Compliance Audit, Self-Certification, Spot Checking, Compliance Investigation, Self-Reporting or Complaint.

Other CIP Standards

The remaining CIP standards follow the same structure as outlined above for CIP 002-5.1a, over 300 pages in the latest Reliability Standards update.⁷ With rare exceptions, the standards eschew technical content in favor of process-oriented guidance. The need for “plans” is dominant, plans take utilities to later decisions on details of the protective mechanisms that ultimately must be acquired, installed, maintained.

Grid-wide Security vs. Individual Utility’s Endpoint Security

Introduction

Since total protection for the Grid depends on the sum of protection for all the facilities labeled “Electronic Secure Perimeter”, it is fair to assess each such facility as an **“end point”**. The security industry frequently characterizes their guidance in terms of either the enterprise, or the users **“endpoint”**, the latter a physical or virtual location with boundary conditions that allow for specific protection advice. For “Grid”



⁵ Section 4.2.1 identifies one or more facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

⁶ The Reliability Assessment Initiative (RAI), a cornerstone of the Compliance process, keys the latter totally to BES Risk Management; permitting self-analysis, and non-public reporting, ostensibly to encourage utilities to open collaboration with CEAs. The RAI has made compliance non-threatening but FERC continues to question NERC efforts to make Compliance totally non-public.

⁷ NERC Reliability Standards for the Bulk Electric Systems of North America, Updated January 3, 2018

security, we must understand that the Grid involves three major, semi-independent segments overseen by independent authorities, the Bulk Electric System (BES), the NRC nuclear generation facilities, and state-controlled distribution facilities. Neither FERC nor NERC (the Industry Reliability Organization) deny this fundamental segregation and can focus cybersecurity oversight only on the BES and its reliability in supporting the entire national electric system.

However, cybersecurity standards or processes do not apply to the Grid as a whole; instead apply to individual utilities engaged primarily in operation of the Bulk Electric System. Grid-wide situational awareness depends almost totally on the interaction of eight BES “Reliability” regions that monitor system operational technologies (OT) to keep the transmission backbone of the Grid functioning, including supporting power generation systems. CIP v5/v6/v7 cybersecurity standards apply separately (and not interactively) to over 1400 “Responsible Entities”, i.e., its accumulated facilities. Each such physical facility is defined as an “**electronic security perimeter** or **ESP**, an “**Endpoint**”. Thus Grid-wide operational cybersecurity rests on the premise that the sum of the Endpoint parts secures the overall BES and that a secured BES protects nuclear sites and massive distribution facilities.

Comment: Would any other major nation-wide enterprise, for example a national security organization, a financial conglomerate, a national healthcare provider, trust its enterprise-wide security totally to individual endpoints? Enterprise-wide security is the major reason why public cloud firms are creating national (and global) VPNs, **coupling** secured virtualized data centers, i.e., securing individual endpoints is simply insufficient to protect the entire, networked enterprise.

Discussion

As directed in Federal law, mainly the 2005 amendment to the Federal Power Act, and subsequent embodiment of Critical Infrastructure Protection standards developed by NERC and implemented by FERC, survivability of the entire national electric system therefore depends on the resiliency of the BES to attack, which in turn depends on the security of most of its core 1400 CIP-protected Endpoints. And those endpoints must survive without benefit of an enterprise-wide operational cybersecurity program; i.e., a 24/7 attack detection/warning/alerting system linking them together.

So the critical question for survival of the nation’s electric system is “Does EndPoint Security for perimeterized utilities protect the BES and therefore assure reliable electrical supply to nuclear sites, and the mass of Distribution Systems serving fifty states and their urban centers?” Forrester, a major Research firm, rates assessments of the performance of 14 top-rated EndPoint Security Companies on three fundamental product/services capabilities - Prevention, Detection, and Remediation. How well are these functions embodied in CIP v5/v6 standards, becomes the major issue:

- Prevention.** Do CIP standards require endpoint systems that prevent malware and exploits from executing; does the suite create an environment where malware cannot, for example, load into memory or stop an exploit from taking advantage of a running process? Do endpoint systems implemented under CIP standards reduce the attack surface through system hardening and applications control?

- Detection.** Do CIP standards ensure that endpoint systems detect malicious activity, post-execution, (knowing attackers will inevitably bypass prevention controls)? For example, do endpoint suites monitor running memory, internal networks, and applications to prevent malware from achieving its goals? Do endpoint systems monitor both process behavior and user behavior to create a context for

complete analysis? Do CIP Standards require a SIEM (Security Incident and Event Monitoring) capability that links all facility security protections to feed comprehensive security management?

•**Remediation.** Do CIP standards result in endpoint security suites that identify and contain malicious endpoint activity or a potential vulnerability? Are endpoint suites capable of launching automated remediation (without significant admin involvement) such as: execution/file quarantining, configuration roll-back? Do they implement blocking actions for process and user behavior?

Assessment

The concept for CIP v5/v6/v7 Standards is one of “Risk/Management”, with Cyber Assets grouped into Cyber Systems in estimating low, medium or high impact loss on the functioning of the Bulk Electric System as a whole. This concept must assume homogeneity of Cyber Assets with strong mutual exclusion features that eliminate major dependencies among Cyber Systems. Otherwise, significant uncontrollable linkages across low, medium and high impact Cyber Systems would make a nonsense of these categories and therefore “Risk Management”.

However, CIP standards as promulgated, seldom specify, or even generalize, on modern interlocking endpoint technical controls such as outlined by Forrester above. CIP standards seldom extend beyond elementary cybersecurity hygienics; e.g., port blocking, password characteristics, personnel accesses, logs, etc., with a complete absence of Endpoint-wide SIEM. Further, there are major exceptions to CIP standards that result, almost always for a given utility, in fuzzy and porous security boundaries and vulnerabilities (for example, data flows) that violate the very concept of endpoint security, such as:

- Mass exclusion from CIP standards of most cyber assets in generation facilities and substations rated below a floor of 300 mw/kva; many with direct internet connectivity and with connectivity to medium and high cyber assets. Also excluded is any facility whose loss would not affect the BES within 15 minutes.
- Complete exclusion from categorization as Cyber assets of all communications and networks linking facility “security perimeters” as defined in CIP v5/v6/v7 standards. (Note that FERC has introduced a contradiction with an Order No. 822 task for development of a standard governing communications security of links between “Control Centers”).
- Near complete absence of CIP standards for acquisition, remote maintenance and operation of modern cyber-vulnerable substation instrumentation systems; programmable logic controllers (PLCs) and other industrial control systems (ICS), synchrophasor control units and related data consolidation centers, and SCADA systems. And more importantly, the cyber infrastructures that link these operational technologies together and generate massive data sets for analysis in facility Energy Management Systems (EMS).

Conclusion

CIP Standards do not link even indirectly to vulnerabilities, and they fail to offset cyber threats that are being experienced. CIP Standards perpetuate a fallacy that “Electronic Secure Perimeters” for individual utilities collectively but imperfectly functioning as cybersecurity endpoints, secure the BES. This is eerily reminiscent of Hadrian’s Wall during the Roman era in England. Hundreds of forts did not contain the Scots. Communications and networking and “Supply Chains” lacked defenses. It took the Romans 400 years to realize they were on an

island and the natives had no place to go. And 1400+ individual utility “ESPs” created from current CIP standards cannot obscure the major vulnerabilities in the North American Grid and their exploitation by Russia’s cyber combat forces.

Exhibit D
To May 11, 2020 Complaint
Submitted by Michael Mabee



MENU

Unfettered Blog

Control Systems Cybersecurity Expert, Joseph M. Weiss, is an international authority on cybersecurity, control systems and system security. Weiss weighs in on cybersecurity, science and technology, security emerging threats and more.

An Assessment of Presidential Executive Order 13920 – Securing the United States Bulk-Power System

Submitted by [Joe Weiss](#) on Mon, 05/04/2020 - 11:59

I do not know what precipitated the issuance of the May 1st, 2020 Executive Order. However, this new Executive Order is long overdue, and addresses many longstanding concerns. The Executive Order demonstrates a high level of technical details and detailed knowledge of existing gaps and vulnerabilities in bulk power equipment and Operations including identifying a specific minimum bulk power voltage level. As a result, the Executive Order will reopen much needed dialogue to address security and policy issues between regulators, policy makers, manufacturers (OEMs) and owner/operators. More specifically, we can expect to see a growing debate on authorities and responsibilities between the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), the Nuclear Regulatory Commission (NRC), etc. Additionally, the Executive Order will directly challenge core NERC Critical Infrastructure Protection (CIP) cyber security requirements that previously excluded the specific bulk electric equipment identified in the Executive Order. Conversely, much of the equipment in scope for the NERC CIPs and supply chain requirements are explicitly identified as out-of-scope for the Executive Order. If the intent is to secure the Bulk Electric Systems with a more balanced approach to securing networking (IT/Operational Technology-OT) and engineering systems, this Executive Order is on target and represents a more comprehensive approach to securing the grid.

China and Russia have directly attacked the control system vendor supply chains since at least 2010. Many of the systems exploited and affected by adversaries are still used in the U.S. bulk and distribution power systems. Moreover, vendors supplying bulk (and distribution) electric equipment for the U.S. electric system also supplied similar (often the same) bulk and distribution electric equipment to other countries, including China, Iran, Russia, and Pakistan. (I include distribution systems, as it often uses the same equipment as transmission systems, and transmission directly “talks” to distribution – more discussions on distribution follows). Even bulk power equipment manufactured in the U.S. often use servers, processors, software, etc. that come from China which makes assuring supply chain integrity so difficult.

Concerns about the bulk power system and its supply chain aren’t new. I had occasion to write, on Wednesday, April 29, 2020, a blog about the lack of cyber security in the electric grid - <https://www.controlglobal.com/blogs/unfettered/energycentral-article-the-continuing-gap-in-control-system-cybersecurity-of-the-electric-industry/>. The blog stated: “I helped start the control system cyber security program for the electric industry in 2000 while at the Electric Power Research Institute-EPRI (I left EPRI in 2002). The program was based on three pillars – physical security (“guns, gates, and guards”) which already existed, network security (needed to be addressed by the IT community), and control system cyber security (which can only be addressed by the control system community including the electric utilities). The program was about “keeping lights on and water flowing”. Keeping Internet Protocol (routable) networks available was not the ultimate goal.”



eBook: Level Measurement Part II

[Latest trends, technology and implementations](#)

Control

Specific to the Executive Order, May 30, 2019, I wrote about counterfeit transmitters - <https://www.controlglobal.com/blogs/unfettered/the-ultimate-control-system-cyber-security-nightmare-using-process-transmitters-as-trojan-horses/>. Counterfeit transmitters from China were making their way into the North American market and the major sensor vendors (not just one) were affected. These counterfeit devices were, and continue to be, a significant safety issue. August 6, 2019, I wrote about the July 25-26, 2019 Cyber War Games at the US Naval War College which a number of major US electric utilities, NERC, and many government organizations participated (representatives from FERC and NRC were not

there) -<https://www.controlglobal.com/blogs/unfettered/the-gap-between-war-games-and-reality-observations-from-the-2019-naval-war-college-cyber-war-game/>. **The issue of “counterfeit SCADA parts” was introduced into the exercise by the Red Team (attackers) resulting in the acting President of the United States (POTUS) issuing a grid security emergency declaration.** The Executive Order is essentially a replay of the July Cyber War Games. Is there a direct correlation? I do not know though there were many from the military and intelligence community participating. Additionally, much of the technical input in the Executive Order looks very familiar.

While I applaud the Executive Order as a major step forward, there remains a significant gap surrounding the security and resilience of local distribution. This is a legacy problem going back to 1996, when FERC deregulated the electric utilities. Securing bulk power must be followed up by tackling the gaps and vulnerabilities associated with processes, technology and policies associated with local distribution if we are to ultimately create a more secure and resilient electric grid. Case in point, a simple example explains this quandary. An electron is “generated” in a power plant and then follows the path of least resistance onto various high voltage transmission lines to lower voltage distribution lines to your house, factory, or military base. There is no way to track the individual electron. The converse can be true. The electron is “generated” on your rooftop solar system and then follows the path of least resistance onto the local distribution electric lines and potentially onto higher voltage transmission lines. The electrons, like the hackers don’t have organization charts to follow or regulations to meet. Yet, the defenders have refused to address this obvious cyber security gap.

Another glimmer of hope is from the Executive Order is that it touches upon more than just the U.S. Bulk Electric systems. The author’s deep understanding of the complexity of the Energy Grid were made apparent by requiring consultation with the Oil and Natural Gas Subsector Coordinating Council in developing the recommendations and evaluation. This is important as one type of equipment explicitly identified in the Executive Order is Safety Instrumented Systems (SIS). Bulk Power Systems, whether nuclear or fossil, do not use SIS, but SIS are used throughout Oil and Natural Gas for process safety. In fact, I am working with two others on a joint process safety/cyber security standard for the process sensor and sensing systems used in SIS.

If the Executive Order does nothing more than provide a coherent approach to identifying and assessing the scope and scale of adversary presence in the U.S. energy sector, it will have achieved a key national security objective that has eluded us for more than a decade. If it brings a more balanced approach and collaboration between IT/OT cyber security investment and plant engineers and operators, we will have added to that success. If the Executive Order further creates new measures of confidence in our committees and measures of performance in security and protection against adversary intrusion and exploitation, it will be a landmark achievement for this administration. That is because "adversaries" (China, Russia, etc.) are on many U.S. and international bulk and distribution standards committees (e.g., IEEE, ISA, ASME, IEC, CIGRE, etc.) as well as policy/research organizations (e.g., the Edison Electric Institute -EEl, EPRI, etc.).

The issues being addressed are not new. The Executive Order is long overdue if we want to "keep the lights on" and "water flowing". I testified before several Congressional committees on these issues starting in 2007. Some of these issues are described in my book – [Protecting Industrial Control Systems from Electronic Threats](#) that was published in 2010. Many policy, technical, and commercial issues associated with cyber security of the electric grid require reconsideration, including, as we have discovered, the participation and leadership of the engineering community.

For further discussion, please contact me at joe.weiss@realtimeacs.com



We're delivering the experts and insights from Smart Industry Base Camp directly to you with the Base Camp Digital series.

Smart industry
BASE CAMP **DIGITAL**

The banner features a dark blue background on the left and an orange background on the right. The text is white and blue. The logo for "Smart industry" is in a smaller font, while "BASE CAMP" is in a large, bold, blue font. "DIGITAL" is in a smaller, blue font with a stylized orange triangle above it.

Joe Weiss

Exhibit E
To May 11, 2020 Complaint
Submitted by Michael Mabee

MENU

Unfettered Blog

Control Systems Cybersecurity Expert, Joseph M. Weiss, is an international authority on cybersecurity, control systems and system security. Weiss weighs in on cybersecurity, science and technology, security emerging threats and more.

Emergency Executive Order 13920 – Response to a real nation-state cyberattack against the US grid

Submitted by [Joe Weiss](#) on Mon, 05/11/2020 - 08:46

This is a follow-up to my May 4th blog on Presidential Executive Order 13920 - <https://www.controlglobal.com/blogs/unfettered/an-assessment-of-presidential-executive-order-13920-securing-the-united-states-bulk-power-system/>

The Executive Order (EO) was issued through emergency powers to address a **real** nation-state cyberattack against the US bulk electric system. The EO is necessary to not only provide the needed cyber security and safety that has been missing from the NERC CIP process and plug the holes in the NERC Supply Chain Program, but to address a real current threat to our country. The NERC CIPs have missed the problems described below and effectively prevented the right people and expertise from being involved which can preclude cyber events (malicious or unintentional) from even being identified. This cannot be allowed to continue.

It is clear the Chinese, Russians, North Koreans, Iranians, etc. have been actively trying to hack into the US grid and other critical infrastructures as well as the control system supply chains for many years. There are acknowledged supply chain issues with critical infrastructure equipment made in the US as they often come with computer chips or software made in China, etc.



eBook: Level Measurement Part II

Latest trends, technology and implementations

Control

The first nation state attack against the US grid is when the Chinese tried to hack into the California Independent System Operator (CA ISO) in 2001. The first case of hacking the control system vendor supply chains were in the 2010-2012 timeframe by China and Russia. The Russians have been in our US grids since 2014. The Chinese were producing counterfeit transmitters in the 2014 timeframe and the counterfeits made their way into North America in the 2018-19 timeframe. Supply chain attacks from China are not just aimed at the US. **I participated in an international power engineering conference where the Chief Engineer from the Power Grid of China described how they were hit by supply chain attacks from within China!**

So why the EO now? Government and public utility procurement rules often push organizations into buying equipment due to price and without regard to origin or risk. In this case, it resulted in a utility having to procure a very large bulk transmission transformer from China. **When the Chinese transformer was delivered to a US utility, the site acceptance testing identified electronics that should NOT have been part of the transformer – hardware backdoors.** That transformer now resides at a government installation. That is why the EO stated: “The Secretary, in consultation with the heads of other agencies as appropriate, may establish and publish criteria for recognizing particular equipment and particular vendors in the bulk-power system electric equipment market as pre-qualified for future transactions; and may apply these criteria to establish and publish a list of pre-qualified equipment and vendors” Procuring a large electric transformer with hardware backdoors is obviously much more significant than having keystroke loggers in Lenovo laptops. An attacker does not install backdoors into a transformer to steal data - you do that to cause damage. It is unclear just how widespread the impact of compromised transformers and other grid equipment are though it is safe to say it is more than just one transformer. Could this be considered an act of war? What does this mean to the 5G discussions about Chinese technology that could affect the electric grid?

The need for having spare transformers started almost 20 years ago because it was recognized these very expensive, long-term procurement items could have a major impact on grid availability. However, unless the devices that are inside or supporting the operation

of the transformers (and generators, motors, valves, capacitor banks, etc.) are also addressed, the pool of spare transformers and other large equipment can be quickly exhausted by damaging the equipment from “within”. As I supported the US Department of Defense (DOD) on the Aurora hardware mitigation program, I am well aware of Aurora and Aurora-type events. Remotely accessing the protective relays can cause an Aurora event damaging the transformer and AC rotating equipment such as generators and motors connected to that substation. **What the Chinese did was install hardware backdoors that can cause an Aurora or other type of damaging event at a time of their choosing.** This is why the list of equipment in the EO is so exhaustive. It also why network devices such as firewalls were not included as they are ineffective with embedded hardware vulnerabilities that can initiate communications from inside the firewall-protected perimeter. It is also why this EO was issued through emergency powers. Addressing this problem requires Engineering to be the lead to address the equipment and devices identified in the EO, not the CISO or OT security organizations, though they should be involved as needed. It also requires changes in procurement requirements.



Build your network.



ControlGlobal.com
PROMOTING EXCELLENCE IN PROCESS AUTOMATION

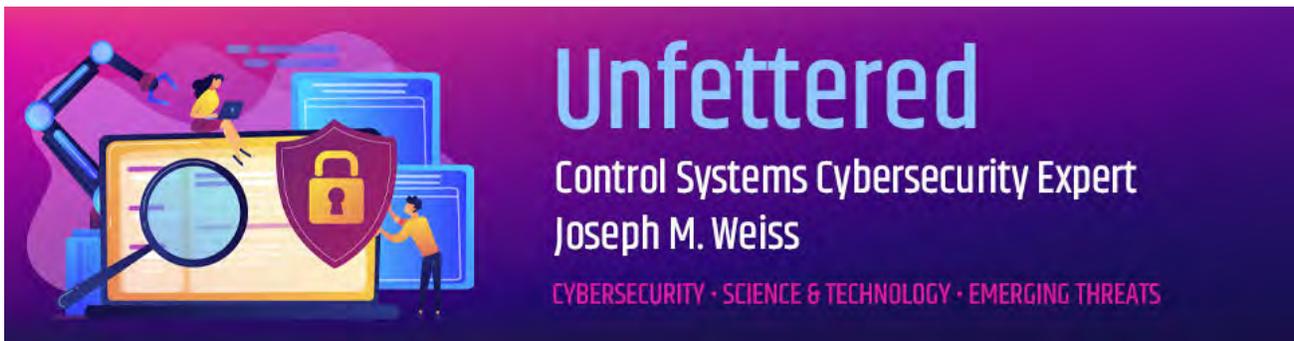


Why are we still buying this critical equipment from China? What does it take to start making them domestically again? Addressing the supply chain is not intractable, but it takes work. For those that cannot assure the supply chain, appropriate monitoring will be key. There is at least one control system vendor, Bedrock Automation (I am on their Technical Advisory Board) that owns their supply chain as they are a spin-off of Maxim Semiconductor. Consequently, securing the supply chain can be done. Work being done by GE and others on advanced equipment monitoring using technology like Digital Ghost can help though there still needs to be monitoring of the sensor and sensing networks independent of the Ethernet Windows displays (more to say in future blogs).

On a separate front, May 6, 2020, Moody's issued their analysis of the EO. The Moody's assessment stated: "US electric utilities will benefit from cybersecurity measures in

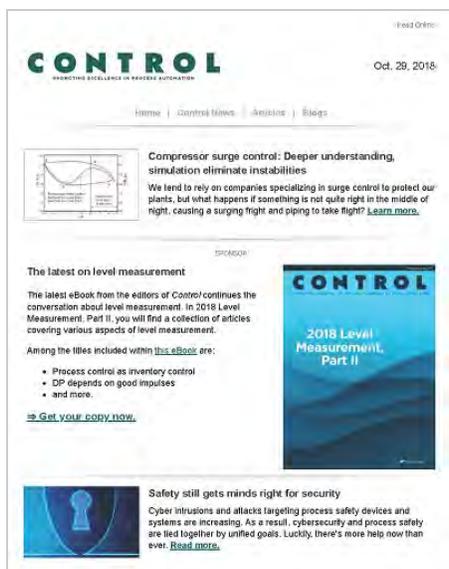
executive order". What the Moody's report implies is if the utilities choose not to address the EO, the impact on their credit ratings will be commensurate.

The EO is necessary to address a real and existing threat. There are financial, technical, and societal needs to embrace the EO. And they have to start now.



Joe Weiss

Like this article? Sign up for the Control newsletters and get articles like this delivered right to your inbox.



Email	*	<input type="text"/>
First Name	*	<input type="text"/>
Last Name	*	<input type="text"/>
Company	*	<input type="text"/>
Country	*	<input type="text" value="Select Country"/>

Sign me up!