116TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
116–256

CYBER SENSE ACT OF 2019

OCTOBER 28, 2019.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. PALLONE, from the Committee on Energy and Commerce, submitted the following

R E P O R T

[To accompany H.R. 360]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 360) to require the Secretary of Energy to establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, and for other purposes, having considered the same, report favorably thereon without amendment and recommend that the bill do pass.

CONTENTS

I. PURPOSE AND SUMMARY

Reps. Robert E. Latta (R–OH) and Jerry McNerney (D–CA) introduced H.R. 360, the "Cyber Sense Act of 2019", on January 9, 2019. The legislation would establish a voluntary U.S. Department of Energy (DOE) program that tests the cybersecurity of products and

technologies intended for use in the bulk-power system, including products related to industrial control systems. The legislation instructs DOE to provide technical assistance to electric utilities, product manufacturers, and other electricity sector stakeholders to help mitigate cybersecurity vulnerabilities. In addition, the bill requires the Secretary of Energy to establish cybersecurity vulnerability reporting processes and maintain a related database.

H.R. 360 requires the Secretary to biennially review products and technologies tested under the Cyber Sense program for cybersecurity vulnerabilities and provide analysis on how such products and technologies respond to and mitigate cyber threats. The legislation instructs the Secretary to develop guidance for electric utilities regarding procurement of products and technologies. The Secretary will utilize analysis and testing results under the Cyber Sense program in developing this guidance.

H.R. 360 directs the Secretary to provide reasonable notice and solicit comments from the public, prior to establishing or revising the Cyber Sense testing process. The legislation provides that any cybersecurity vulnerability reported pursuant to this program, the disclosure of which the Secretary of Energy reasonably foresees would cause harm to critical electric infrastructure, shall be deemed "critical electric infrastructure information" as defined by section 215A(d) of the Federal Power Act. The legislation also includes Federal Government liability protections by noting that nothing shall be construed to authorize the commencement of an action against the United States Government with respect to the testing of a product or technology under the Cyber Sense program.

II. BACKGROUND AND NEED FOR LEGISLATION

The United States energy infrastructure is comprised of a vast network of energy and electricity systems that deliver uninterrupted electricity from producers to consumers. These intricate and highly interdependent systems enable every aspect of our daily lives. Our Nation's economy, security, and the health and safety of its citizens depend upon the reliable and uninterrupted supply of fuels and electricity. Since the inception of the Department of Energy in 1977, the manner in which energy and power is generated, transmitted, and delivered continues to rapidly change and evolve. As advances in digital and information technologies continue to layer onto existing practices and energy infrastructures, new risks emerge, and vulnerabilities are exposed. Recent high-profile attempts by foreign actors to infiltrate our Nation's energy systems and infrastructure further highlight the need for legislation aimed at mitigating these significant and growing threats to the reliable supply of energy in the United States.

The Department of Energy's Authorities for Cybersecurity, Energy Security, and Emergency Response

When the Department of Energy was organized in 1977, energy security concerns revolved around oil supply shortages. As a result, energy security emergency functions in the Department of Energy Organization Act focused on distributing and allocating fuels in an emergency. Over time, while DOE's organic statute remained largely unchanged, its responsibilities and authorities have evolved substantially beyond what was envisioned 40 years ago. Energy deliv-

ery systems have become increasingly interconnected and digitized, while society has become more dependent on energy in all its forms—expanding the opportunities for cybersecurity threats and other hazards that may require emergency response.

Today, the mission of DOE to advance the national, economic, and energy security of the United States requires it to act as the lead agency for the protection of electric power, oil, and natural gas infrastructure. DOE has authority and responsibilities for the physical and cybersecurity of energy delivery systems from laws that Congress has passed and Presidential directives. Congress has provided DOE with a wide range of emergency response and cybersecurity authorities affecting multiple segments of the energy sector, beginning with the Department of Energy Organization Act, and most recently with the Fixing America's Surface Transportation Act (FAST Act).

The FAST Act, which was signed into law in 2015, designated DOE as the Sector-Specific Agency (SSA) for the energy sector and provided the Department with several new energy security authorities to respond to physical and cyberattacks to energy systems. Section 61003 of the FAST Act amended section 215 of the Federal Power Act (FPA) and created a new section 215A entitled, "Critical Electric Infrastructure Security." This new section 215A of the FPA provided definitions for the terms "bulk power system", "critical electric infrastructure", "critical electric infrastructure information", and "grid security emergency" [1] among other terms. Section 215 of the FPA states that when the President issues or provides to the Secretary of Energy a written directive or determination identifying a grid security emergency, the Secretary may, with or without notice, hearing, or report, issue orders for emergency measures to protect or restore the reliability of critical electric infrastructure or of defense critical electric infrastructure during an emergency.[2] Section 215A also includes protections for the sharing of critical electric information.

DOE's cybersecurity roles and responsibilities are also guided by the Federal Government's operational framework, as provided by the Presidential Policy Directive 41 (PPD–41) issued in 2016 addressing "United States Cyber Incident Coordination." A primary purpose of PPD–41 is to improve coordination across the Federal Government by clarifying roles and responsibilities. Under the PPD–41 framework, DOE serves as the lead agency for the energy sector, coordinating closely with other agencies and the private sector to facilitate the response, recovery, and restoration of damaged energy infrastructure.

On February 14, 2018, the Secretary of Energy established a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at DOE. The CESER office is currently led by Assistant

[1] *See* Section 215A of the Federal Power Act, the term "Grid Security Emergency" means the occurrence or imminent danger of (A)(i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure; and (ii) disruption of the operation of such devices or networks, with significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event; or (B)(i) a direct physical attack on critical electric infrastructure or on defense critical electric infrastructure; and (ii) significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.

[2] Federal Power Act § 215A, *16 U.S.C. §§ 824o–1.*

Secretary Karen S. Evans, whose work focuses on energy infrastructure security, supporting the expanded national security responsibilities assigned to DOE and reporting to the Under Secretary of Energy.[3]

Physical Security and Cybersecurity of the Electric Grid

With respect to its responsibilities for security of the electric power system, DOE works closely with electric sector owners and operators to detect and mitigate risks to critical electric infrastructure. DOE collaborates with the electric sector to develop technologies, tools, exercises, and other resources to assist the energy sector in evaluating and improving their security preparedness.[4]

Along with DOE, the Federal Energy Regulatory Commission (FERC) has authority over the reliability of the electric grid. Congress, through the Energy Policy Act of 2005,[5] provided FERC with the authority to approve mandatory cybersecurity standards proposed by the Electric Reliability Organization (ERO). The North American Electric Reliability Corporation (NERC) currently serves as the ERO. NERC proposes reliability standards for planning and operating the North American bulk power system. These critical infrastructure protection (CIP) reliability standards[6] address physical security and cybersecurity of critical electric infrastructure.

Cooperation between the Federal Government and electricity sector extends beyond mandatory and enforceable standards. The Electricity Subsector Coordinating Council (ESCC)[7] serves as the principal liaison between the Federal Government and the electric power sector in coordinating efforts to prepare for national-level incidents or threats to critical infrastructure. The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, funded by DOE and industry. CRISP is managed by the Electricity Information Sharing and Analysis Center (E–ISAC)[8] and facilitates the timely bi-directional sharing of unclassified and classified threat information with energy sector partners.[9]

Need for Legislation to Mitigate against Supply Chain Vulnerabilities

The Committee finds that H.R. 360 would help mitigate against vulnerabilities to supply chains by testing the cybersecurity of products and technologies intended for use in the bulk-power system, as noted in the Committee's legislative record.

The Committee finds that the DOE Cyber Sense program established through H.R. 360 would allow electric utilities and industry stakeholders to have greater awareness of the cybersecurity of products and technologies they utilize in the bulk-power system. Electric utilities and industry stakeholders can help mitigate against vulnerabilities to energy supply chains by making more informed decisions when choosing products and technologies.

---

[3] *See* Press Release, U.S. Department of Energy, "Karen Evans Sworn in as DOE Assistant Secretary for Cybersecurity, Energy Security, and Emergency Response." (Sep. 4, 2018), *https://www.energy.gov/articles/karen-evans-sworn-doe-assistant-secretary-cybersecurity-energy-security-and-emergency.*

[4] Department of Energy. *Energy Sector Cybersecurity Preparedness.*

[5] *P.L. 109–58.*

[6] *See North American Electric Reliability Corporation* for further information.

[7] *See Electric Subsector Coordinating Council* for further information.

[8] *See Electricity Information Sharing and Analysis Center* for further information.

[9] Department of Energy. *Cybersecurity for Critical Energy Infrastructure.*

III. COMMITTEE HEARINGS

For the purposes of section 103(i) of H. Res. 6 of the 116th Congress—(1) the following hearing was used to develop or consider H.R. 360: The Subcommittee on Energy held a hearing on July 12, 2019, entitled Keeping The Lights On: Addressing Cyber Threats To The Grid." The Subcommittee received testimony from the following witnesses:

- Karen S. Evans, Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy;
- J. Andrew Dodge, Sr., Director, Office of Reliability, Federal Energy Regulatory Commission; and
- Jim Robb, President and Chief Executive Officer, North American Electric Reliability Corporation.

IV. COMMITTEE CONSIDERATION

H.R. 360 was introduced in the House of Representatives and referred to the Committee on Energy and Commerce on January 9, 2019. Subsequently, the bill was referred to the Subcommittee on Energy on January 25, 2019. On May 16, 2019, the Subcommittee on Energy met in open markup session, pursuant to notice, to consider H.R. 360 and agreed to a motion by Mr. Rush, Chairman of the Subcommittee, to forward the bill H.R. 360 favorably to the full Committee, without amendment, by a voice vote.

On July 17, 2019, the full Committee on Energy and Commerce met in open markup session, pursuant to notice, to consider H.R. 360. No amendments were offered at full Committee. Subsequently, the Committee agreed to a motion by Mr. Pallone, Chairman, to order the bill H.R. 360 reported favorably to the House, without amendment, by a voice vote, a quorum being present.

V. COMMITTEE VOTES

Clause 3(b) of rule XIII requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto. There were no recorded votes taken in connection with ordering H.R. 360 reported.

VI. OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII and clause 2(b)(1) of rule X of the Rules of the House of Representatives, the oversight findings and recommendations of the Committee are reflected in the descriptive portion of the report.

VII. NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Pursuant to 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

The Committee has requested but not received from the Director of the Congressional Budget Office a statement as to whether this bill contains any new budget authority, spending authority, credit

authority, or an increase or decrease in revenues or tax expenditures.

VIII. FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

IX. STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the general performance goal or objective of this legislation is to require the Secretary of Energy to establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system.

X. DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII, no provision of H.R. 360 is known to be duplicative of another Federal program, including any program that was included in a report to Congress pursuant to section 21 of Public Law 111–139 or the most recent Catalog of Federal Domestic Assistance.

XI. COMMITTEE COST ESTIMATE

Pursuant to clause 3(d)(1) of rule XIII, the Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

XII. EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

Pursuant to clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 360 contains no earmarks, limited tax benefits, or limited tariff benefits.

XIII. ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

XIV. APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

XV. SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section provides that the Act may be cited as the "Cyber Sense Act of 2019".

Section 2. Cyber sense

(a) In general

Section 2(a) states that the Secretary shall establish a voluntary Department of Energy program to test the cybersecurity of products and technologies intended for use in the bulk-power system, as defined by section 215(a) of the Federal Power Act (16 U.S.C. 824o(a)).

(b) Program requirements

Section 2(b) states that the Secretary of Energy, in carrying out subsection (a) shall: (1) establish a testing process under the Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, including products relating to industrial control systems and operational technologies, such as supervisory control and data acquisition systems; (2) for products and technologies tested under the Cyber Sense program, establish and maintain cybersecurity vulnerability reporting processes and a related database; (3) provide technical assistance to electric utilities, product manufacturers, and other electricity sector stakeholders to mitigate identified cybersecurity vulnerabilities.

Under section 2(b)(4) the Secretary shall biennially review products and technologies under the Cyber Sense program for cybersecurity vulnerabilities and provide analysis with respect to how such products and technologies respond to and mitigate cyber threats. Pursuant to section 2(b)(5) the Secretary shall develop guidance, that is informed by analysis and testing results under the Cyber Sense program, for electric utilities for procurement of products and technologies. For section 2(b)(6) the Secretary shall provide reasonable notice to the public, prior to establishing or revising the testing process under the Cyber Sense program.

For section 2(b)(7) the Secretary shall oversee the testing of products and technologies under the Cyber Sense program; and 2(b)(8) consider incentives to encourage the use of analysis and results of testing under the Cyber Sense program in the design of products and technologies for use in the bulk-power system.

(c) Disclosure of information

Under section 2(c) any cybersecurity vulnerability reported pursuant to a process established under subsection (b)(2), the disclosure of which the Secretary of Energy reasonably foresees would cause harm to critical electric infrastructure (as defined in section 215A) of the Federal Power Act, shall be deemed to be critical electric infrastructure information for purposes of section 215A(d) of the Federal Power Act.

(d) Federal Government liability

Section 2(d) states nothing in section 2 shall be construed to authorize the commencement of an action against the United States Government with respect to the testing of a product or technology under the Cyber Sense program.

XVI. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation does not amend any existing Federal statute.

○