AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

116TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
116–254

ENHANCING GRID SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIPS ACT

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. 359]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 359) to provide for certain programs and developments in the Department of Energy concerning the cybersecurity and vulnerabilities of, and physical threats to, the electric grid, and for other purposes, having considered the same, report favorably thereon without amendment and recommend that the bill do pass.

CONTENTS

		Page
I.	Purpose and Summary	1
II.	Background and Need for the Legislation	2
III.	Committee Hearings	5
IV.	Committee Consideration	5
V.	Committee Votes	5
VI.	Oversight Findings	5
VII.	New Budget Authority, Entitlement Authority, and Tax Expenditures	5
VIII.	Federal Mandates Statement	6
IX.	Statement of General Performance Goals and Objectives	6
X.	Duplication of Federal Programs	6
XI.	Committee Cost Estimate	6
XII.	Earmarks, Limited Tax Benefits, and Limited Tariff Benefits	6
XIII.	Advisory Committee Statement	6
XIV.	Applicability to Legislative Branch	6
XV.	Section-by-Section Analysis of the Legislation	7
XVI.	Changes in Existing Law Made by the Bill, as Reported	8

I. PURPOSE AND SUMMARY

Reps. Jerry McNerney (D–CA) and Robert E. Latta (R–OH) introduced H.R. 359, the "Enhancing Grid Security through Public-Private Partnerships Act", on January 9, 2019. This legislation would

require the Department of Energy (DOE) Secretary to establish a program to facilitate and encourage public-private partnerships to promote and advance physical security and cybersecurity of electric utilities.

The Secretary of Energy is directed to carry out a program to (1) develop, and provide for voluntary implementation of, maturity models, self-assessments, and auditing methods for assessing the physical security and cybersecurity of electric utilities; (2) provide training and technical assistance to electric utilities to address and mitigate cybersecurity supply chain management risks; and (3) increase opportunities for sharing best practices and data collection within the electric sector.

The Secretary is also required to take into consideration different sizes of electric utilities and the regions they serve and to prioritize electric utilities with fewer available resources due to size or region. Any information an electric utility provides to the Federal Government through this program will be exempt from public disclosure under Federal, State, or tribal law.

The bill also provides for a report to Congress addressing cybersecurity as it relates to the electric distribution system. H.R. 359 directs the Secretary to assess priorities, policies, procedures, and actions for enhancing the physical and cybersecurity of the electric distribution system, including the costs and benefits of implementing these priorities, policies, procedures, and actions.

Finally, H.R. 359 directs DOE to update the Interruption Cost Estimate Calculator, a tool designed for and utilized by electric reliability planners at electric utilities, government organizations, or other entities that are interested in estimating interruption costs and benefits associated with infrastructure improvements.

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, these functions in DOE's organic statute re-

mained largely unchanged, but DOE's responsibilities and authorities have evolved substantially beyond what was envisioned 40 years ago. Energy delivery 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 DOE mission 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 security 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.

---

[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.

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 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

The Committee finds that section 2 of H.R. 359 would facilitate and strengthen public-private partnerships to promote and advance the physical security and cybersecurity of electric utilities that have fewer resources due to size or region.

The Committee finds section 3 of H.R. 359 would help mitigate against threats and vulnerabilities to electricity distribution systems by assessing priorities, policies, procedures, and actions for enhancing the physical and cybersecurity of electric distribution systems.

---

[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.

The Committee finds section 4 of H.R. 359 would help improve electric infrastructure resilience by updating a program that assists grid planners at utilities, government organizations and other entities with estimating interruption costs and benefits associated with infrastructure improvements.

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. 359: 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. 359 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. 359 and agreed to a motion by Mr. Rush, Chairman of the Subcommittee, to forward the bill H.R. 359 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. 359. No amendments were offered at full Committee. Subsequently, the Committee agreed to a motion by Mr. Pallone, Chairman, to order the bill H.R. 359 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. 359 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 rev-

enues 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 provide programs and developments in the Department of Energy concerning the cybersecurity and vulnerabilities of, and physical threats to, the electric grid, and for other purposes.

X. DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII, no provision of H.R. 359 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. 359 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 "Enhancing Grid Security through Public-Private Partnerships Act".

Section 2. Program to promote and advance physical security and cybersecurity of electric utilities

(a) Establishment

The Secretary of Energy, in consultation with State regulatory authorities, industry stakeholders, and other Federal agencies the Secretary determines appropriate, shall carry out a program to (1) develop, and provide for voluntary implementation of, maturity models, self-assessments, and auditing methods for assessing the physical security and cybersecurity of electric utilities; (2) provide training and technical assistance to electric utilities to address and mitigate cybersecurity supply chain management risks; (3) increase opportunities for sharing best practices and data collection within the electric sector; (4) assist with cybersecurity training for electric utilities; (5) advance the cybersecurity of third-party vendors that work in partnerships with electric utilities; and (6) provide technical assistance for electric utilities subject to the program.

(b) Scope

Section 2(b) states that in carrying out the program under section 2(a), the Secretary of Energy shall (1) take into consideration different sizes of electric utilities and the regions that such electric utilities serve; (2) prioritize electric utilities with fewer available resources due to size or region; and (3) to the extent practicable, utilize and leverage existing Department of Energy programs.

(c) Protection of information

Section 2(c) states that information provided to, or collected by, the Federal Government pursuant to this section, (1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and (2) shall not be made available by any Federal, State, political subdivision, or tribal law requiring disclosure of information or records.

Section 3. Report on cybersecurity and distribution systems

(a) In general

Section 3(a) directs the Secretary of Energy, in consultation with State regulatory authorities, industry stakeholders, and other Federal agencies the Secretary determines appropriate, shall submit to Congress a report that assesses (1) priorities, policies, procedures, and actions for enhancing the physical security and cybersecurity of electricity distribution systems to address threats to, and vulnerabilities of, such electricity distribution systems. Section 3(a)(2) further clarifies that this report will assess implementation of such priorities, policies, procedures, and actions, including an estimate of potential costs and benefits of such implementation, including any public-private cost-sharing opportunities.

(b) Protection of information

Section 3(b) states that information provided to, or collected by, the Federal Government pursuant to this section, (1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and (2) shall not be made available by any Federal, State, political subdivision, or tribal law requiring disclosure of information or records.

Section 4. Electricity interruption information

(a) Interruption Cost Estimate Calculator

Section 4(a) directs that the Secretary of Energy, in consultation with the Federal Energy Regulatory Commission, State regulatory authorities, industry stakeholders, and other Federal agencies the Secretary determines appropriate, shall update the Interruption Cost Estimate Calculator, as often as appropriate and feasible, but not less than once every 2 years.

(b) Indices

Section 4(b) instructs that the Secretary of Energy, in consultation with the Federal Energy Regulatory Commission, State regulatory authorities, industry stakeholders, and other Federal agencies the Secretary determines appropriate, shall, as often as appropriate and feasible, update the following: (1) The System Average Interruption Duration Index; (2) The System Average Interruption Frequency Index; and (3) The Customer Average Interruption Index.

(c) Survey

Section 4(c) directs that the Administrator of the Energy Information Administration shall collect information on electricity interruption costs, if available, from a representative sample of owners of electric grid assets through biennial survey.

Section 5. Definitions

For this legislation the term "electric utility" has the meaning given such term in section 3 of the Federal Power Act (16 U.S.C. 796). The term "State regulatory authority" has the meaning given such term in section 3 of the Federal Power Act (16 U.S.C. 796).

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

This legislation does not amend any existing Federal statute.

○