115TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
115–794

CYBER SENSE ACT OF 2018

JUNE 28, 2018.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

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

R E P O R T

[To accompany H.R. 5239]

[Including cost estimate of the Congressional Budget Office]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 5239) to require the Secretary of Energy to establish a voluntary Cyber Sense program to identify and promote cyber-secure products intended for use in the bulk-power system, and for other purposes, having considered the same, report favorably thereon with amendments and recommend that the bill as amended do pass.

CONTENTS

The amendments are as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cyber Sense Act of 2018".

SEC. 2. CYBER SENSE.

(a) IN GENERAL.—The Secretary of Energy shall establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, as defined in section 215(a) of the Federal Power Act (16 U.S.C. 824o(a)).

(b) PROGRAM REQUIREMENTS.—In carrying out subsection (a), the Secretary of Energy 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 develop solutions to mitigate identified cybersecurity vulnerabilities in products and technologies tested under the Cyber Sense program;

(4) biennially review products and technologies tested 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;

(5) develop guidance, that is informed by analysis and testing results under the Cyber Sense program, for electric utilities for procurement of products and technologies;

(6) provide reasonable notice to the public, and solicit comments from the public, prior to establishing or revising the testing process under the Cyber Sense program;

(7) oversee testing of products and technologies under the Cyber Sense program; and

(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.—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.—Nothing in this section 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.

Amend the title so as to read:

A bill 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.

PURPOSE AND SUMMARY

H.R. 5239, Cyber Sense Act of 2018, was introduced by Rep. Robert Latta (R–OH) and Rep. Jerry McNerney (D–CA) on March 9, 2018. H.R. 5239 would establish a voluntary 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. 5239 requires the Secretary to review biennially 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. 5239 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.

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 forty 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, DOE's 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 in-

frastructure. 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 Energy Secretary established a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at DOE. The CESER office will be led by an Assistant Secretary that will focus on energy infrastructure security, support the expanded national security responsibilities assigned to DOE, and report to the Under Secretary of Energy.[3]

---

[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.

[3] *See* Press Release, U.S. Department of Energy, "Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response." (Feb. 14, 2018), https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency.

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. 5239 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. According to the testimony of Undersecretary Mark Menezes, "[s]ecuring the electric sector supply chain is critical to the security and resilience of the electric grid. Products must be tested for known vulnerabilities in order to assess risk and develop mitigations."[10]

The testimony of Kyle Pistor, Vice President of Government Relations for the National Electrical Manufacturers Association (NEMA) was supportive of the bill and discussed the need and importance of securing energy supply chains to better protect the nation's electric grid. Mr. Pistor noted, "[s]upply chain disruption and compromise are major concerns for the electric utility industry, and

[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.
[10] *See* Written Testimony of Under Secretary Mark Menezes, U.S. Department of Energy, Before the Subcommittee on Energy, Committee on Energy and Commerce, March 14, 2018.

both electric utilities and manufacturers."[11] Mr. Pistor also stated, "[m]ember manufacturers support voluntary cybersecurity evaluation of products used in the transmission, distribution, storage, and end-use of electricity. Not doing so could permit unsecure equipment to be installed, potentially compromising the electric system."[12] Mr. Pistor provided several recommendations regarding the collaboration and participation of manufacturers involved with the Cyber Sense program.

The Committee finds that the DOE Cyber Sense program established through H.R. 5239 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.

COMMITTEE ACTION

On March 14, 2018, the Subcommittee on Energy held a legislative hearing on H.R. 5239 entitled "DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response." The Subcommittee received testimony from:

- Mark Menezes, Under Secretary of Energy, U.S. Department of Energy;
- Scott Aaronson, Vice President, Security and Preparedness, Edison Electric Institute;
- Mark Engels, Senior Enterprise Security Advisor, Dominion Energy;
- Tristan Vance, Director, Office of Energy Development, State of Indiana;
- Zachary Tudor, Associate Laboratory Director for National and Homeland Security, Idaho National Laboratory; and,
- Kyle Pistor, Vice President of Government Relations, National Electrical Manufactures Association.

On April 18, 2018, the Subcommittee on Energy met in open markup session and forwarded H.R. 5239, as amended, to the full Committee by a voice vote.

On May 9, 2018, the full Committee on Energy and Commerce met in open markup session and ordered H.R. 5239, as amended, favorably reported to the House by a voice vote.

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. 5239 reported.

---

[11] *See* Written Testimony of Mr. Kyle Pistor, Vice President, Government Relations for the National Electrical Manufacturers Association, Before the Subcommittee on Energy, Committee on Energy and Commerce, March 14, 2018.

[12] *See* Written Testimony of Mr. Kyle Pistor, Vice President, Government Relations for the National Electrical Manufacturers Association, Before the Subcommittee on Energy, Committee on Energy and Commerce, March 14, 2018.

OVERSIGHT FINDINGS AND RECOMMENDATIONS

Pursuant to clause 2(b)(1) of rule X and clause 3(c)(1) of rule XIII, the Committee has held a hearing and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Pursuant to clause 3(c)(2) of rule XIII, the Committee finds that H.R. 5239 would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, May 18, 2018.

Hon. GREG WALDEN,
Chairman, Committee on Energy and Commerce,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5239, the Cyber Sense Act of 2018.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Megan Carroll.

Sincerely.

MARK P. HADLEY
(For Keith Hall, Director).

Enclosure.

H.R. 5239—Cyber Sense Act of 2018

Summary: H.R. 5239 would direct the Department of Energy (DOE) to establish a program to identify and promote products and technologies to mitigate the threat of cyber-related disruptions to the bulk power system. (The bulk power system comprises facilities and control systems necessary for operating an interconnected network for transmitting electric energy and facilities that generate electricity necessary to maintain the reliability of that network.)

CBO estimates that implementing H.R. 5239 would cost $56 million over the 2019–2023 period, assuming appropriation of the necessary amounts. Enacting the bill would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

CBO estimates that enacting H.R. 5239 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

H.R. 5239 would impose an intergovernmental mandate, as defined in the Unfunded Mandates Reform Act (UMRA), on state, local, and tribal governments, but CBO estimates that it would impose no duty on those governments that would result in additional spending or a loss of revenues.

H.R. 5239 contains no private-sector mandates as defined in UMRA.

Estimated cost to the Federal Government: The estimated budgetary effect of H.R. 5239 is shown in the following table. The costs of the legislation fall primarily within budget function 270 (energy).

	By fiscal year, in millions of dollars—						
	2018	2019	2020	2021	2022	2023	2019–2023
INCREASES IN SPENDING SUBJECT TO APPROPRIATION							
Estimated Authorization Level	0	15	15	16	16	16	78
Estimated Outlays	0	3	9	12	16	16	56

Basis of estimate: H.R. 5239 would direct DOE to establish a voluntary program for testing the cybersecurity of products and technologies intended for use in the bulk power system. The bill would specify requirements for that program and direct the agency to provide guidance and technical assistance, using information and analysis from the proposed testing program, to stakeholders of the electricity sector to help mitigate cybersecurity vulnerabilities.

Using information from DOE, CBO estimates that implementing H.R. 5239 would cost $56 million over the 2019–2023 period. That estimate is based on the Administration's cost estimates for activities that DOE has proposed to carry out that are similar to those in the bill, and it reflects historical spending patterns for activities administered by DOE's Office of Electricity.

Pay-As-You-Go considerations: None.

Increase in long-term direct spending and deficits: CBO estimates that enacting H.R. 5239 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

Mandates: H.R. 5239 would impose an intergovernmental mandate, as defined in UMRA, on state, local, and tribal governments. The bill would preempt state and local laws that could otherwise cause governmental agencies participating in the proposed program to disclose information about their activities, such as the sharing of cybersecurity information.

Although the preemption would limit the application of state and local laws, CBO estimates that it would impose no duty on state or local governments that would result in additional spending or a loss of revenue.

H.R. 5239 contains no private-sector mandates as defined in UMRA.

Estimate prepared by: Federal costs: Megan Carroll; Mandates: Jon Sperl.

Estimate reviewed by: Kim P. Cawley, Chief, Natural and Physical Resources Cost Estimates Units; Susan Willie, Chief, Mandates Unit; H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

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.

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.

DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII, no provision of H.R. 5239 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.

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.

EARMARK, 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. 5239 contains no earmarks, limited tax benefits, or limited tariff benefits.

DISCLOSURE OF DIRECTED RULE MAKINGS

Pursuant to section 3(i) of H. Res. 5, the Committee finds that H.R. 5239 contains no directed rule makings.

ADVISORY COMMITTEE STATEMENT

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

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.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section provides the short title of "Cyber Sense Act of 2018."

Section 2. Cyber Sense

Section 2(a) states that the Secretary shall establish a voluntary Department of Energy (DOE) 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)).

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 prod-

ucts 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 paragraph (5), the Secretary shall develop guidance for electric utilities for procurement of products and technologies. The guidance shall be informed by analysis and testing results under the Cyber Sense program. For paragraph (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 (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.

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.

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.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation does not amend any existing Federal statute.

○