115TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 115–951
Part 1

PIPELINE AND LNG FACILITY CYBERSECURITY PREPAREDNESS ACT

SEPTEMBER 13, 2018.—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. 5175]

[Including cost estimate of the Congressional Budget Office]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 5175) to require the Secretary of Energy to carry out a program relating to physical security and cybersecurity for pipelines and liquefied natural gas facilities, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Pipeline and LNG Facility Cybersecurity Preparedness Act".

SEC. 2. PHYSICAL SECURITY AND CYBERSECURITY FOR PIPELINES AND LIQUEFIED NATURAL GAS FACILITIES.

The Secretary of Energy, in carrying out the Department of Energy's functions pursuant to the Department of Energy Organization Act (42 U.S.C. 7101 et seq.), and in consultation with appropriate Federal agencies, representatives of the energy sector, the States, and other stakeholders, shall carry out a program—

(1) to establish policies and procedures to coordinate Federal agencies, States, and the energy sector, including through councils or other entities engaged in sharing, analysis, or sector coordinating, to ensure the security, resiliency, and survivability of natural gas pipelines (including natural gas transmission and distribution pipelines), hazardous liquid pipelines, and liquefied natural gas facilities;

(2) to coordinate response and recovery by Federal agencies, States, and the energy sector, to physical incidents and cyber incidents impacting the energy sector;

(3) to develop, for voluntary use, advanced cybersecurity applications and technologies for natural gas pipelines (including natural gas transmission and distribution pipelines), hazardous liquid pipelines, and liquefied natural gas facilities;

(4) to perform pilot demonstration projects relating to physical security and cybersecurity for natural gas pipelines (including natural gas transmission and distribution pipelines), hazardous liquid pipelines, and liquefied natural gas facilities with representatives of the energy sector;

(5) to develop workforce development curricula for the energy sector relating to physical security and cybersecurity for natural gas pipelines (including natural gas transmission and distribution pipelines), hazardous liquid pipelines, and liquefied natural gas facilities; and

(6) to provide technical tools to help the energy sector voluntarily evaluate, prioritize, and improve physical security and cybersecurity capabilities of natural gas pipelines (including natural gas transmission and distribution pipelines), hazardous liquid pipelines, and liquefied natural gas facilities.

SEC. 3. SAVINGS CLAUSE.

Nothing in this Act shall be construed to modify the authority of any Federal agency other than the Department of Energy relating to physical security or cybersecurity for natural gas pipelines (including natural gas transmission and distribution pipelines), hazardous liquid pipelines, or liquefied natural gas facilities.

PURPOSE AND SUMMARY

H.R. 5175, Pipeline and LNG Facility Cybersecurity Preparedness Act, was introduced by Rep. Fred Upton (R–MI) and Rep. David Loebsack (D–IA) on March 6, 2018. H.R. 5175 requires the Secretary of Energy to carry out a program to coordinate among Federal agencies, States, and the energy sector to ensure the security, resiliency, and survivability of natural gas pipelines, hazardous liquid pipelines, and liquefied natural gas facilities.

H.R. 5175 also requires the Secretary to coordinate response and recovery to physical and cyber incidents impacting the energy sector, develop advanced cybersecurity applications and technologies, perform pilot demonstration projects, develop workforce development curricula relating to physical and cybersecurity, and provide mechanisms to help the energy sector evaluate, prioritize, and improve physical and cybersecurity capabilities.

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 (DOE) 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 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

[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

Continued

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 who will focus on energy infrastructure security, support the expanded national security responsibilities assigned to DOE, and report to the Under Secretary of Energy.[3]

Physical security and cybersecurity for pipeline and LNG facilities

As the Energy SSA, DOE is required to coordinate with multiple Federal and State agencies and collaborate with energy infrastructure owners and operators on activities associated with identifying vulnerabilities and mitigating incidents that may impact the energy sector. To perform these duties effectively, DOE must account for each interrelated segment of the nation's energy infrastructure, including pipelines, which are subject to an array of other Federal authorities. In a January 24, 2018 letter, the Committee wrote to Secretary Perry to better understand the level of coordination among governmental agencies.[4] In response, Secretary Perry noted that "a coordinated government approach to the cyber and physical security of pipelines, led by the Department of Energy, is essential to ensuring the safe and reliable flow of energy across the U.S."[5]

The Committee finds that H.R. 5175 would improve the quality of coordination among the various Federal entities relating to cybersecurity of the nation's pipeline system, as noted in the Committee's legislative hearing record. According to testimony of DOE Undersecretary Mark Menezes, "the Department is focusing cyber support efforts to enhance visibility and situational awareness of operational networks; increase alignment of cyber preparedness

---

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.

[4] See Letter from Chairman Greg Walden to Secretary Rick Perry dated January 24, 2018, available at: https://energycommerce.house.gov/wp-content/uploads/2018/01/20180124DOE.pdf.

[5] See Letter from Secretary Rick Perry to Chairman Greg Walden dated March 13, 2018, available at: https://docs.house.gov/meetings/IF/IF03/20180314/107999/HHRG-115-IF03-20180314-SD053.pdf.

and planning across local, state, and Federal levels; and leverage the expertise of DOE's National Labs to drive cybersecurity innovation."[6] The Committee finds that H.R. 5175 would support and enhance these efforts.

The Committee finds that H.R. 5175 would also allow DOE to improve collaboration with the energy sector and the States to build capacity to mitigate cyber threats. The testimony of Mark Engels, Senior Enterprise Security Advisor for Dominion Energy, was generally supportive of efforts to improve the focus on pipeline cybersecurity and physical security and coordination efforts. Mr. Engels noted that "while natural gas pipeline operators have a general idea about how the relevant Federal agencies associated with pipeline security should work together, H.R. 5175 would ideally encourage clarification on the issue." Mr. Engels also provided examples where Dominion Energy successfully collaborated with DOE and the National Labs to test industrial control systems, identify supply chain threats, and improve equipment procurement processes.

The purpose of H.R. 5175 is to clarify DOE's role and responsibility within the existing cyber incident command framework as the SSA for the Energy Sector.

H.R. 5175 does not authorize a regulatory program and does not duplicate existing cybersecurity or safety mandates issued by DHS or DOT. H.R. 5175 clarifies that DOE's advanced cybersecurity applications, technologies, and technical tools developed are for voluntary use.

H.R. 5175 also includes a savings clause to clarify that nothing in the Act shall be construed to modify the authority of any other Federal agency relating to physical security or cybersecurity for pipelines or liquefied natural gas facilities.

COMMITTEE ACTION

On March 14, 2018 the Subcommittee on Energy held a hearing on H.R. 5175 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. 5175, as amended, to the full Committee by a voice vote.

[6] 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.

On May 9, 2018, the full Committee on Energy and Commerce met in open markup session and ordered H.R. 5175, 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. 5175 reported.

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. 5175 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, June 6, 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. 5175, the Pipeline and LNG Facility Cybersecurity Preparedness Act.

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

Sincerely,

KEITH HALL,
Director.

Enclosure.

H.R. 5175—Pipeline and LNG Facility Cybersecurity Preparedness Act

Summary: H.R. 5175 would direct the Department of Energy (DOE) to undertake a variety of activities aimed at improving the physical security and cybersecurity of pipelines and liquid natural gas (LNG) facilities.

CBO estimates that implementing H.R. 5175 would cost $86 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. 5175 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

H.R. 5175 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA).

Estimated cost to the Federal Government: The estimated budgetary effect of H.R. 5175 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	29	28	18	18	18	111
Estimated Outlays	0	7	17	20	22	20	86

Basis of estimate: H.R. 5175 would require DOE, in consultation with other federal agencies, states, representatives of the energy sector, and other stakeholders, to pursue activities related to the physical security and cybersecurity of pipelines and LNG facilities. The bill would direct DOE to perform pilot projects to test and demonstrate security-related technologies. It also would specify DOE's role in coordinating federal, state, and private entities' responses to and recoveries from physical and cyber incidents that affect the energy sector. H.R. 5175 also would authorize DOE to establish safety criteria related to workforce development and provide technical assistance to the energy sector.

Assuming appropriation of the necessary amounts, CBO estimates that implementing H.R. 5175 would require appropriations totaling $111 million over the 2019–2023 period. Using information from DOE about the costs of similar activities, CBO expects DOE would need most of that amount—$95 million—to develop the physical infrastructure necessary to support pilot projects to test security-related technology under the bill. Based on spending patterns for similar activities, CBO estimates that outlays would total $70 million over the 2019–2023 period, with the remainder spending after 2013.

CBO also estimates that, under H.R. 5175, DOE's administrative costs would increase by $16 million—primarily for three or four additional staff needed to meet the agency's expanded role related to the physical security of pipelines and LNG facilities, added costs to establish databases and information-sharing systems, and to provide additional technical assistance to the energy sector. CBO estimates that all of those funds would be spent over the 2019–2023 period.

Pay-As-You-Go considerations: None.

Increase in long-term direct spending and deficits: CBO estimates that enacting H.R. 5175 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. 5175 contains no intergovernmental or 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 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 carry out a program relating to physical security and cybersecurity for pipelines and liquified natural gas facilities.

DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII, no provision of H.R. 5175 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. 5175 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

Section 1 provides the short title of "Pipeline and LNG Facility Cybersecurity Preparedness Act."

Section 2. Physical security and cybersecurity for pipelines and liquefied natural gas facilities

Section 2 requires the Secretary of Energy to carry out a program focused on physical security and cybersecurity for natural gas and hazardous liquid pipelines and LNG facilities. Section 2 requires DOE to consult with appropriate Federal agencies, representatives of the energy sector, the States, and other stakeholders to establish policies and procedures to improve coordination; develop advanced cybersecurity applications and technologies; perform pilot demonstrations; develop workforce development curricula; and, to provide technical tools to improve physical security and cybersecurity capabilities.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation does not amend any existing Federal statute.

○