116TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 116–303
Part 1

PIPELINE AND LNG FACILITY CYBERSECURITY PREPAREDNESS ACT

NOVEMBER 20, 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. 370]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 370) 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 without amendment and recommend that the bill do pass.

CONTENTS

I. PURPOSE AND SUMMARY

Reps. Fred Upton (R–MI) and David Loebsack (D–IA) introduced H.R. 370, the "Pipeline and LNG Facility Cybersecurity Preparedness Act", on January 9, 2019. H.R. 370 requires the Department

of Energy (DOE) Secretary to carry out a program to coordinate 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. 370 also requires the Secretary of Energy to coordinate response and recovery to physical and cyber incidents affecting 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.

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 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 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 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 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 affect the energy sector. To perform these duties effectively, DOE must account for each interrelated segment of the Nation's energy infrastructure, in-

[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, "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.

cluding pipelines, which are subject to an array of other Federal authorities.

Along with DOE, the Transportation Security Administration (TSA) has responsibility related to security for pipelines. According to the Congressional Research Service (CRS), the Aviation and Transportation Security Act of 2001, which established the Transportation Security Administration within the U.S. Department of Transportation, authorized the agency "to issue, rescind, and revise such regulations as are necessary" to carry out its functions.[4] TSA was transferred to the Department of Homeland Security, which was created under the Homeland Security Act of 2002.[5] The Implementing Recommendations of the 9/11 Commission Act of 2007 directs TSA to promulgate pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate.[6]

The Committee finds that H.R. 370 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 legislative hearing record.

The Committee finds that H.R. 370 would also allow DOE to improve collaboration with the energy sector and the States to build capacity to mitigate cyber threats.

The purpose of H.R. 370 is to clarify roles and responsibilities, improve collaboration and build capacity within States and the energy sector, and accelerate research and development of advanced cybersecurity tools and technologies. The Committee finds that H.R. 370 would improve the ability of DOE to coordinate with other agencies and participate within the existing cyber incident command framework as the SSA for the Energy Sector.

H.R. 370 does not authorize a regulatory program and it is not intended to duplicate existing cybersecurity or safety mandates issued by DHS or DOT. H.R. 370 clarifies that the advanced cybersecurity applications, technologies, and technical tools developed are for voluntary use.

H.R. 370 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.

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. 370: 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, United States Department of Energy;
- J. Andrew Dodge, Sr., Director, Office of Reliability, Federal Energy Regulatory Commission; and

[4] P.L. 107–71.
[5] P.L. 107–296.
[6] P.L. 110–53.

• Jim Robb, President and Chief Executive Officer, North American Electric Reliability Corporation.

IV. COMMITTEE CONSIDERATION

H.R. 370 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. 370 and agreed to a motion by Mr. Rush, Chairman of the Subcommittee, to forward the bill H.R. 370 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. 370. No amendments were offered at full Committee. Subsequently, the Committee agreed to a motion by Mr. Pallone, Chairman, to order the bill H.R. 370 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. 370 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 En-

ergy to carry out a program relating to physical security and cybersecurity for pipelines and liquified natural gas facilities.

X. DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII, no provision of H.R. 370 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. 370 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

Section 1 provides that the Act may be cited as the "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.

Section 3. Savings clause

Section 3 provides that nothing in this Act shall be construed to modify the authority of any Federal agency other that DOE relat-

ing to physical security or cybersecurity for natural gas pipelines, including transmission and distribution pipelines, hazardous liquid pipelines, or liquefied natural gas facilities.

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

This legislation does not amend any existing Federal statute.

○