Calendar No. 410

115TH CONGRESS
2D SESSION

S. 79

[Report No. 115–246]

To provide for the establishment of a pilot program to identify security vulnerabilities of certain entities in the energy sector.

IN THE SENATE OF THE UNITED STATES

JANUARY 10, 2017

Mr. KING (for himself, Mr. RISCH, Mr. HEINRICH, Ms. COLLINS, and Mr. CRAPO) introduced the following bill; which was read twice and referred to the Committee on Energy and Natural Resources

MAY 10, 2018

Reported by Ms. MURKOWSKI, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

To provide for the establishment of a pilot program to identify security vulnerabilities of certain entities in the energy sector.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

~~**SECTION 1. SHORT TITLE.**~~

~~This Act may be cited as the ''Securing Energy Infrastructure Act''.~~

SEC. 2. DEFINITIONS.

In this Act:

(1) COVERED ENTITY.—The term ''covered entity'' means an entity identified pursuant to section 9(a) of Executive Order 13636 of February 12, 2013 (78 Fed. Reg. 11742) relating to identification of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

(2) EXPLOIT.—The term ''exploit'' means a software tool designed to take advantage of a security vulnerability.

(3) INDUSTRIAL CONTROL SYSTEM.—

(A) IN GENERAL.—The term ''industrial control system'' means an operational technology used to measure, control, or manage industrial functions.

(B) INCLUSIONS.—The term ''industrial control system'' includes supervisory control and data acquisition systems, distributed control systems, and programmable logic or embedded controllers.

(4) NATIONAL LABORATORY.—The term ''National Laboratory'' has the meaning given the term

in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(5) PROGRAM.—The term ''Program'' means the pilot program established under section 3.

(6) SECRETARY.—The term ''Secretary'' means the Secretary of Energy.

(7) SECURITY VULNERABILITY.—The term ''security vulnerability'' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

SEC. 3. PILOT PROGRAM FOR SECURING ENERGY INFRASTRUCTURE.

Not later than 180 days after the date of enactment of this Act, the Secretary shall establish a 2-year control systems implementation pilot program within the National Laboratories for the purposes of—

(1) partnering with covered entities in the energy sector (including critical component manufacturers in the supply chain) that voluntarily participate in the Program to identify new classes of security vulnerabilities of the covered entities; and

(2) researching, developing, testing, and implementing technology platforms and standards, in partnership with covered entities, to isolate and defend industrial control systems of covered entities

from security vulnerabilities and exploits in the most critical systems of the covered entities, including—

(A) analog and non-digital control systems;

(B) purpose-built control systems; and

(C) physical controls.

SEC. 4. WORKING GROUP.

(a) ESTABLISHMENT.—The Secretary shall establish a working group—

(1) to evaluate the technology platforms and standards used in the Program under section 3(2); and

(2) to develop a national cyber-informed engineering strategy to isolate and defend covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities.

(b) MEMBERSHIP.—The working group established under subsection (a) shall be composed of not fewer than 10 members, to be appointed by the Secretary, at least 1 member of which shall represent each of the following:

(1) The Department of Energy.

(2) The energy industry, including electric utilities and manufacturers recommended by the Energy Sector coordinating councils.

(3)(A) The Department of Homeland Security; or

(B) the Industrial Control Systems Cyber Emergency Response Team.

(4) The North American Electric Reliability Corporation.

(5) The Nuclear Regulatory Commission.

(6)(A) The Office of the Director of National Intelligence; or

(B) the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

(7)(A) The Department of Defense; or

(B) the Assistant Secretary of Defense for Homeland Security and America's Security Affairs.

(8) A State or regional energy agency.

(9) A national research body or academic institution.

(10) The National Laboratories.

SEC. 5. REPORT.

Not later than 2 years after the date on which funds are first disbursed under the Program, the Secretary shall submit to the appropriate committees of Congress a final report that—

(1) describes the results of the Program;

(2) includes an analysis of the feasibility of each method studied under the Program; and

(3) describes the results of the evaluations conducted by the working group established under section 4(a).

SEC. 6. NO NEW REGULATORY AUTHORITY.

Nothing in this Act authorizes the Secretary or the head of any other Federal agency to issue new regulations.

SEC. 7. EXEMPTION FROM DISCLOSURE.

Information shared by or with the Federal Government or a State, tribal, or local government under this Act shall be—

(1) deemed to be voluntarily shared information; and

(2) exempt from disclosure under any provision of Federal, State, tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring the disclosure of information or records.

SEC. 8. PROTECTION FROM LIABILITY.

(a) IN GENERAL.—A cause of action against a covered entity for engaging in the voluntary activities authorized under section 3—

(1) shall not lie or be maintained in any court; and

(2) shall be promptly dismissed by the applicable court.

~~(b) VOLUNTARY ACTIVITIES.—Nothing in this Act subjects any covered entity to liability for not engaging in the voluntary activities authorized under section 3.~~

~~SEC. 9. AUTHORIZATION OF APPROPRIATIONS.~~

~~(a) PILOT PROGRAM.—There is authorized to be appropriated $10,000,000 to carry out section 3.~~

~~(b) WORKING GROUP AND REPORT.—There is authorized to be appropriated $1,500,000 to carry out sections 4 and 5.~~

~~(c) AVAILABILITY.—Amounts made available under subsections (a) and (b) shall remain available until expended.~~

SECTION 1. SHORT TITLE.

This Act may be cited as the "Securing Energy Infrastructure Act".

SEC. 2. DEFINITIONS.

In this Act:

(1) APPROPRIATE COMMITTEE OF CONGRESS.—The term "appropriate committee of Congress" means—

(A) the Select Committee on Intelligence, the Committee on Homeland Security and Governmental Affairs, and the Committee on Energy and Natural Resources of the Senate; and

(B) the Permanent Select Committee on Intelligence, the Committee on Homeland Security, and the Committee on Energy and Commerce of the House of Representatives.

(2) COVERED ENTITY.—The term "covered entity" means an entity identified pursuant to section 9(a) of Executive Order 13636 of February 12, 2013 (78 Fed. Reg. 11742), relating to identification of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

(3) EXPLOIT.—The term "exploit" means a software tool designed to take advantage of a security vulnerability.

(4) INDUSTRIAL CONTROL SYSTEM.—

(A) IN GENERAL.—The term "industrial control system" means an operational technology used to measure, control, or manage industrial functions.

(B) INCLUSIONS.—The term "industrial control system" includes supervisory control and data acquisition systems, distributed control systems, and programmable logic or embedded controllers.

(5) NATIONAL LABORATORY.—The term "National Laboratory" has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(6) PROGRAM.—The term "Program" means the pilot program established under section 3.

(7) SECRETARY.—The term "Secretary" means the Secretary of Energy.

(8) SECURITY VULNERABILITY.—The term "security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

SEC. 3. PILOT PROGRAM FOR SECURING ENERGY INFRASTRUCTURE.

Not later than 180 days after the date of enactment of this Act, the Secretary shall establish a 2-year control systems implementation pilot program within the National Laboratories for the purposes of—

(1) partnering with covered entities in the energy sector (including critical component manufacturers in the supply chain) that voluntarily participate in the Program to identify new classes of security vulnerabilities of the covered entities; and

(2) evaluating technology and standards, in partnership with covered entities, to isolate and de-

fend industrial control systems of covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities, including—

(A) analog and nondigital control systems;

(B) purpose-built control systems; and

(C) physical controls.

SEC. 4. WORKING GROUP TO EVALUATE PROGRAM STANDARDS AND DEVELOP STRATEGY.

(a) ESTABLISHMENT.—The Secretary shall establish a working group—

(1) to evaluate the technology and standards used in the Program under section 3(2); and

(2) to develop a national cyber-informed engineering strategy to isolate and defend covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities.

(b) MEMBERSHIP.—The working group established under subsection (a) shall be composed of not fewer than 10 members, to be appointed by the Secretary, at least 1 member of which shall represent each of the following:

(1) The Department of Energy.

(2) The energy industry, including electric utilities and manufacturers recommended by the Energy Sector coordinating councils.

(3)(A) The Department of Homeland Security; or

(B) the Industrial Control Systems Cyber Emergency Response Team.

(4) The North American Electric Reliability Corporation.

(5) The Nuclear Regulatory Commission.

(6)(A) The Office of the Director of National Intelligence; or

(B) the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

(7)(A) The Department of Defense; or

(B) the Assistant Secretary of Defense for Homeland Security and America's Security Affairs.

(8) A State or regional energy agency.

(9) A national research body or academic institution.

(10) The National Laboratories.

SEC. 5. REPORTS ON THE PROGRAM.

(a) INTERIM REPORT.—Not later than 180 days after the date on which funds are first disbursed under the Program, the Secretary shall submit to the appropriate committees of Congress an interim report that—

(1) describes the results of the Program;

(2) includes an analysis of the feasibility of each method studied under the Program; and

(3) describes the results of the evaluations conducted by the working group established under section 4(a).

(b) FINAL REPORT.—Not later than 2 years after the date on which funds are first disbursed under the Program, the Secretary shall submit to the appropriate committees of Congress a final report that—

(1) describes the results of the Program;

(2) includes an analysis of the feasibility of each method studied under the Program; and

(3) describes the results of the evaluations conducted by the working group established under section 4(a).

SEC. 6. EXEMPTION FROM DISCLOSURE.

Information shared by or with the Federal Government or a State, Tribal, or local government under this Act shall be—

(1) deemed to be voluntarily shared information;

(2) exempt from disclosure under section 552 of title 5, United States Code, or any provision of any State, Tribal, or local freedom of information law, open government law, open meetings law, open

records law, sunshine law, or similar law requiring the disclosure of information or records; and

(3) withheld from the public, without discretion, under section 552(b)(3) of title 5, United States Code, or any provision of a State, Tribal, or local law requiring the disclosure of information or records.

SEC. 7. PROTECTION FROM LIABILITY.

(a) IN GENERAL.—A cause of action against a covered entity for engaging in the voluntary activities authorized under section 3—

(1) shall not lie or be maintained in any court; and

(2) shall be promptly dismissed by the applicable court.

(b) VOLUNTARY ACTIVITIES.—Nothing in this Act subjects any covered entity to liability for not engaging in the voluntary activities authorized under section 3.

SEC. 8. NO NEW REGULATORY AUTHORITY FOR FEDERAL AGENCIES.

Nothing in this Act authorizes the Secretary or the head of any other department or agency of the Federal Government to issue new regulations.

SEC. 9. AUTHORIZATION OF APPROPRIATIONS.

(a) PILOT PROGRAM.—There is authorized to be appropriated $10,000,000 to carry out section 3.

(b) WORKING GROUP AND REPORT.—There is authorized to be appropriated $1,500,000 to carry out sections 4 and 5.

(c) AVAILABILITY.—Amounts made available under subsections (a) and (b) shall remain available until expended.

Calendar No. 410

115TH CONGRESS
2D SESSION

S. 79

[Report No. 115–246]

A BILL

To provide for the establishment of a pilot program to identify security vulnerabilities of certain entities in the energy sector.

MAY 10, 2018

Reported with an amendment