

Calendar No. 264

116TH CONGRESS }
1st Session }

SENATE

{ REPORT
116-144

ENERGY CYBERSECURITY ACT OF 2019

OCTOBER 23, 2019.—Ordered to be printed

Ms. MURKOWSKI, from the Committee on Energy and Natural Resources, submitted the following

R E P O R T

[To accompany S. 2333]

The Committee on Energy and Natural Resources, to which was referred the bill (S. 2333) to provide for enhanced energy grid security, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

PURPOSE

The purpose of S. 2333 is to provide for enhanced energy grid security.

BACKGROUND AND NEED

The United States' electric grid is comprised of a vast network of transmission and distribution systems that deliver electricity from producers to consumer homes and businesses. Many sectors of our economy, including healthcare and manufacturing, simply cannot operate without a reliable supply of electricity. As advances in digital and information technology continue to electrify our daily lives, we increase our exposure to a potentially devastating cyber or physical attack on the grid.

A number of federal agencies are responsible for protecting our electric grid from physical and cyber threats, including DOE and the Federal Energy Regulatory Commission (FERC). DOE works closely with electric sector owners and operators to detect and mitigate risks to critical electric infrastructure, and to develop tools and other resources to assist the sector in evaluating and improving their security preparedness. Also, with the enactment of the Fixing America's Surface Transportation Act (Public Law 114-94)

in 2015, Congress codified DOE as the Sector-Specific Agency for cybersecurity for the energy sector.

With respect to FERC, the Energy Policy Act of 2005 (Public Law 109–58) created the Electric Reliability Organization (ERO) to develop mandatory reliability standards for the electric transmission system, including physical and cybersecurity standards. The law tasked FERC with approving and enforcing these mandatory standards—violations of which that can result in penalties of up to \$1 million per violation per day.

S. 2333 would establish a program at DOE to develop advanced energy cybersecurity technologies, secure control system vulnerabilities, and develop workforce curricula for energy sector cybersecurity. The bill would also establish a program to identify and address supply chain vulnerabilities and expand the cooperation of the Federal government with industry to coordinate responses to cyber threats.

LEGISLATIVE HISTORY

S. 2333 was introduced by Senators Cantwell and Heinrich on July 30, 2019.

In the 115th Congress, a similar measure was included as section 2002 in S. 1460, the Energy and Natural Resources Act of 2017. S. 1460 was introduced by Senators Murkowski and Cantwell on June 28, 2017, and placed directly on the Legislative Calendar (Cal. 162).

In the 114th Congress, a similar measure was included as section 2002 in S. 2012, the Energy Policy Modernization Act of 2016. An original bill, S. 2012 was reported by the Committee on Energy and Natural Resources on July 30, 2015, and passed by the Senate, as amended, on April 26, 2016, by a vote of 85–12.

The Senate Committee on Energy and Natural Resources met in open business session on September 25, 2019, and ordered S. 2333 favorably reported.

COMMITTEE RECOMMENDATION

The Senate Committee on Energy and Natural Resources, in open business session on September 25, 2019, by a majority voice vote of a quorum present, recommends that the Senate pass S. 2333. Senators Barrasso and Lee asked to be recorded as voting no.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

Section 1 sets forth the short title of the bill.

Sec. 2. Definitions

Section 2 provides key definitions.

Sec. 3. Enhanced grid security

Section 3(a) directs the Secretary of Energy (Secretary) to carry out a program to develop advanced energy sector cybersecurity technologies and applications, and to leverage electric grid architecture to assess risks to the energy sector. It further authorizes \$65 million for each of fiscal years (FYs) 2020 through 2028 to carry out subsection (a).

Subsection (b) requires the Secretary to carry out a program on cybertesting and mitigation to identify vulnerabilities of energy sector supply chain products; oversee third-party cybertesting; and develop procurement guidelines for energy sector supply chain components. It further authorizes \$15 million for each of FYs 2020 through 2028 to carry out subsection (b).

Subsection (c) authorizes the Secretary to carry out a program on energy sector operational support for cyberresilience with the following objectives: to enhance and periodically test the emergency response capabilities of the Department and coordination with the Department, the National Laboratories, and private industry; expand cooperation of DOE with the intelligence community for energy sector-related threat collection; enhance the tools of the DOE and the Electricity Information Sharing and Analysis Center (E-ISAC) for monitoring the status of the energy sector; expand industry participation in E-ISAC; and provide technical assistance to small electric utilities to assess cybermaturity. It further authorizes \$10 million for each of FYs 2020 through 2028 to carry out subsection (c).

Subsection (d) directs the Secretary to develop an advanced energy security program to secure energy networks. The program's objective is to increase the functional preservation of electric grid operations or natural gas and oil operations in the face of threats and hazards. In carrying out this program the Secretary is authorized to develop capabilities to identify vulnerabilities; provide modeling to predict impacts; develop a maturity model for physical and cybersecurity; conduct exercises to mitigate electric grid vulnerabilities; conduct research for electric grid components; and provide technical assistance for standards and risk analysis. It further authorizes \$10 million for each of FYs 2020 through 2028 to carry out subsection (d).

Subsection (e) requires the program to be carried out consistent with existing Department programs, DOE's 2011 "Roadmap to Achieve Energy Delivery Systems Cybersecurity," and any other relevant strategic framework.

Subsection (f) directs the Secretary, in consultations with FERC and the North American Electric Reliability Corporation, to conduct a study within 180 days of enactment to explore alternative management structures and funding mechanisms to expand industry participation in E-ISAC, and to submit such study to the appropriate Congressional committees.

COST AND BUDGETARY CONSIDERATIONS

The Congressional Budget Office estimate of the costs of this measure has been requested but was not received at the time the report was filed. When the Congressional Budget Office completes its cost estimate, it will be posted on the internet at www.cbo.gov.

REGULATORY IMPACT EVALUATION

In compliance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee makes the following evaluation of the regulatory impact which would be incurred in carrying out S. 2333. The bill is not a regulatory measure in the sense of imposing Government-established standards or significant economic responsibilities on private individuals and businesses.

No personal information would be collected in administering the program. Therefore, there would be no impact on personal privacy.

Little, if any, additional paperwork would result from the enactment of S. 2333, as ordered reported.

CONGRESSIONALLY DIRECTED SPENDING

S. 2333, as ordered reported, does not contain any congressionally directed spending items, limited tax benefits, or limited tariff benefits as defined in rule XLIV of the Standing Rules of the Senate.

EXECUTIVE COMMUNICATIONS

Executive views on S. 2333 were not requested by the Committee.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, the Committee notes that no changes in existing law are made by S. 2333 as ordered reported.