(E) to advance, in partnership with electric utilities, the cybersecurity of third-party vendors that manufacture components of the electric grid;

(F) to increase opportunities for sharing best practices and data collection within the electric sector; and

(G) to assist, in the case of electric utilities that own defense critical electric infrastructure (as defined in section 824*o*–1(a) of title 16), with full engineering reviews of critical functions and operations at both the utility and defense infrastructure levels—

(i) to identify unprotected avenues for cyber-enabled sabotage that would have catastrophic effects to national security; and

(ii) to recommend and implement engineering protections to ensure continued operations of identified critical functions even in the face of constant cyber attacks and achieved perimeter access by sophisticated adversaries.

(2) Scope

In carrying out the program under paragraph (1), the Secretary shall—

(A) take into consideration—

(i) the different sizes of electric utilities; and

(ii) the regions that electric utilities serve;

(B) prioritize electric utilities with fewer available resources due to size or region; and

(C) to the maximum extent practicable, use and leverage—

(i) existing Department and Department of Homeland Security programs; and

(ii) existing programs of the Federal agencies determined to be appropriate under paragraph (1).

(c) Report on cybersecurity of distribution systems

Not later than 1 year after November 15, 2021, the Secretary, in coordination with the Secretary of Homeland Security and in consultation with, as the Secretary determines to be appropriate, the heads of other Federal agencies, State regulatory authorities, and industry stakeholders, shall submit to Congress a report that assesses—

(1) priorities, policies, procedures, and actions for enhancing the physical security and cybersecurity of electricity distribution systems, including behind-the-meter generation, storage, and load management devices, to address threats to, and vulnerabilities of, electricity distribution systems; and

(2) the implementation of the priorities, policies, procedures, and actions assessed under paragraph (1), including—

(A) an estimate of potential costs and benefits of the implementation; and

(B) an assessment of any public-private cost-sharing opportunities.

(d) Protection of information

Information provided to, or collected by, the Federal Government pursuant to this section the disclosure of which the Secretary reasonably foresees could be detrimental to the physical security or cybersecurity of any electric utility or the bulk-power system—

(1) shall be exempt from disclosure under section 552(b)(3) of title 5; and

(2) shall not be made available by any Federal agency, State, political subdivision of a State, or Tribal authority pursuant to any Federal, State, political subdivision of a State, or Tribal law, respectively, requiring public disclosure of information or records.

(Pub. L. 117–58, div. D, title I, § 40121, Nov. 15, 2021, 135 Stat. 949.)

Statutory Notes and Related Subsidiaries

WAGE RATE REQUIREMENTS

For provisions relating to rates of wages to be paid to laborers and mechanics on projects for construction, alteration, or repair work funded under div. D or an amendment by div. D of Pub. L. 117–58, including authority of Secretary of Labor, see section 18851 of this title.

§ 18722. Energy cyber sense program

(a) Definitions

In this section:

(1) Bulk-power system

The term ''bulk-power system'' has the meaning given the term in section 824*o*(a) of title 16.

(2) Program

The term ''program'' means the voluntary Energy Cyber Sense program established under subsection (b).

(b) Establishment

The Secretary, in coordination with the Secretary of Homeland Security and in consultation with the heads of other relevant Federal agencies, shall establish a voluntary Energy Cyber Sense program to test the cybersecurity of products and technologies intended for use in the energy sector, including in the bulk-power system.

(c) Program requirements

In carrying out subsection (b), the Secretary, in coordination with the Secretary of Homeland Security and in consultation with the heads of other relevant Federal agencies, shall—

(1) establish a testing process under the program to test the cybersecurity of products and technologies intended for use in the energy sector, 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 program, establish and maintain cybersecurity vulnerability reporting processes and a related database that are integrated with Federal vulnerability coordination processes;

(3) provide technical assistance to electric utilities, product manufacturers, and other energy sector stakeholders to develop solutions to mitigate identified cybersecurity vulnerabilities in products and technologies tested under the program;

(4) biennially review products and technologies tested under the program for

cybersecurity vulnerabilities and provide analysis with respect to how those products and technologies respond to and mitigate cyber threats;

(5) develop guidance that is informed by analysis and testing results under the program for electric utilities and other components of the energy sector for the procurement of products and technologies;

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

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

(8) consider incentives to encourage the use of analysis and results of testing under the program in the design of products and technologies for use in the energy sector.

(d) Protection of information

Information provided to, or collected by, the Federal Government pursuant to this section the disclosure of which the Secretary reasonably foresees could be detrimental to the physical security or cybersecurity of any component of the energy sector, including any electric utility or the bulk-power system—

(1) shall be exempt from disclosure under section 552(b)(3) of title 5; and

(2) shall not be made available by any Federal agency, State, political subdivision of a State, or Tribal authority pursuant to any Federal, State, political subdivision of a State, or Tribal law, respectively, requiring public disclosure of information or records.

(e) Federal Government liability

Nothing in this section authorizes the commencement of an action against the United States with respect to the testing of a product or technology under the program.

(Pub. L. 117–58, div. D, title I, § 40122, Nov. 15, 2021, 135 Stat. 950.)

Statutory Notes and Related Subsidiaries

Wage Rate Requirements

For provisions relating to rates of wages to be paid to laborers and mechanics on projects for construction, alteration, or repair work funded under div. D or an amendment by div. D of Pub. L. 117–58, including authority of Secretary of Labor, see section 18851 of this title.

§ 18723. Rural and municipal utility advanced cybersecurity grant and technical assistance program

(a) Definitions

In this section:

(1) Advanced cybersecurity technology

The term ''advanced cybersecurity technology'' means any technology, operational capability, or service, including computer hardware, software, or a related asset, that enhances the security posture of electric utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat (as defined in section 650 of title 6).

(2) Bulk-power system

The term ''bulk-power system'' has the meaning given the term in section 824*o*(a) of title 16.

(3) Eligible entity

The term ''eligible entity'' means—

(A) a rural electric cooperative;

(B) a utility owned by a political subdivision of a State, such as a municipally owned electric utility;

(C) a utility owned by any agency, authority, corporation, or instrumentality of 1 or more political subdivisions of a State;

(D) a not-for-profit entity that is in a partnership with not fewer than 6 entities described in subparagraph (A), (B), or (C); and

(E) an investor-owned electric utility that sells less than 4,000,000 megawatt hours of electricity per year.

(4) Program

The term ''Program'' means the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program established under subsection (b).

(b) Establishment

Not later than 180 days after November 15, 2021, the Secretary, in coordination with the Secretary of Homeland Security and in consultation with the Federal Energy Regulatory Commission, the North American Electric Reliability Corporation, and the Electricity Subsector Coordinating Council, shall establish a program, to be known as the ''Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program'', to provide grants and technical assistance to, and enter into cooperative agreements with, eligible entities to protect against, detect, respond to, and recover from cybersecurity threats.

(c) Objectives

The objectives of the Program shall be—

(1) to deploy advanced cybersecurity technologies for electric utility systems; and

(2) to increase the participation of eligible entities in cybersecurity threat information sharing programs.

(d) Awards

(1) In general

The Secretary—

(A) shall award grants and provide technical assistance under the Program to eligible entities on a competitive basis;

(B) shall develop criteria and a formula for awarding grants and providing technical assistance under the Program;

(C) may enter into cooperative agreements with eligible entities that can facilitate the objectives described in subsection (c); and

(D) shall establish a process to ensure that all eligible entities are informed about and can become aware of opportunities to receive grants or technical assistance under the Program.

(2) Priority for grants and technical assistance

In awarding grants and providing technical assistance under the Program, the Secretary