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

shall give priority to an eligible entity that, as determined by the Secretary—

(A) has limited cybersecurity resources;

(B) owns assets critical to the reliability of the bulk-power system; or

(C) owns defense critical electric infrastructure (as defined in section 824*o*–1(a) of title 16).

(e) 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.

(f) Authorization of appropriations

There is authorized to be appropriated to the Secretary to carry out this section $250,000,000 for the period of fiscal years 2022 through 2026.

(Pub. L. 117–58, div. D, title I, § 40124, Nov. 15, 2021, 135 Stat. 953; Pub. L. 117–263, div. G, title LXXI, § 7143(d)(3), Dec. 23, 2022, 136 Stat. 3663.)

Editorial Notes

AMENDMENTS

2022—Subsec. (a)(1). Pub. L. 117–263 substituted ''section 650 of title 6'' for ''section 1501 of title 6''.

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.

§ 18724. Enhanced grid security

(a) Definitions

In this section:

(1) Electric utility

The term ''electric utility'' has the meaning given the term in section 796 of title 16.

(2) E-ISAC

The term ''E-ISAC'' means the Electricity Information Sharing and Analysis Center.

(b) Cybersecurity for the energy sector research, development, and demonstration program

(1) In general

The Secretary, in coordination with the Secretary of Homeland Security and in consultation with, as determined appropriate, other Federal agencies, the energy sector, the States, Indian Tribes, Tribal organizations, territories or freely associated states, and other stakeholders, shall develop and carry out a program—

(A) to develop advanced cybersecurity applications and technologies for the energy sector—

(i) to identify and mitigate vulnerabilities, including—

(I) dependencies on other critical infrastructure;

(II) impacts from weather and fuel supply;

(III) increased dependence on inverter-based technologies; and

(IV) vulnerabilities from unpatched hardware and software systems; and

(ii) to advance the security of field devices and third-party control systems, including—

(I) systems for generation, transmission, distribution, end use, and market functions;

(II) specific electric grid elements including advanced metering, demand response, distribution, generation, and electricity storage;

(III) forensic analysis of infected systems;

(IV) secure communications; and

(V) application of in-line edge security solutions;

(B) to leverage electric grid architecture as a means to assess risks to the energy sector, including by implementing an all-hazards approach to communications infrastructure, control systems architecture, and power systems architecture;

(C) to perform pilot demonstration projects with the energy sector to gain experience with new technologies;

(D) to develop workforce development curricula for energy sector-related cybersecurity; and

(E) to develop improved supply chain concepts for secure design of emerging digital components and power electronics.

(2) Authorization of appropriations

There is authorized to be appropriated to the Secretary to carry out this subsection $250,000,000 for the period of fiscal years 2022 through 2026.

(c) Energy sector operational support for cyberresilience program

(1) In general

The Secretary may develop and carry out a program—

(A) to enhance and periodically test—

(i) the emergency response capabilities of the Department; and

(ii) the coordination of the Department with other agencies, the National Laboratories, and private industry;

(B) to expand cooperation of the Department with the intelligence community for energy sector-related threat collection and analysis;

(C) to enhance the tools of the Department and E-ISAC for monitoring the status of the energy sector;

(D) to expand industry participation in E-ISAC; and