(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.)

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

(E) to provide technical assistance to small electric utilities for purposes of assessing and improving cybermaturity levels and addressing gaps identified in the assessment.

(2) Authorization of appropriations

There is authorized to be appropriated to the Secretary to carry out this subsection $50,000,000 for the period of fiscal years 2022 through 2026.

(d) Modeling and assessing energy infrastructure risk

(1) In general

The Secretary, in coordination with the Secretary of Homeland Security, shall develop

and carry out an advanced energy security program to secure energy networks, including—

(A) electric networks;

(B) natural gas networks; and

(C) oil exploration, transmission, and delivery networks.

(2) Security and resiliency objective

The objective of the program developed under paragraph (1) is to increase the functional preservation of electric grid operations or natural gas and oil operations in the face of natural and human-made threats and hazards, including electric magnetic pulse and geomagnetic disturbances.

(3) Eligible activities

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

(A) develop capabilities to identify vulnerabilities and critical components that pose major risks to grid security if destroyed or impaired;

(B) provide modeling at the national level to predict impacts from natural or human-made events;

(C) add physical security to the cybersecurity maturity model;

(D) conduct exercises and assessments to identify and mitigate vulnerabilities to the electric grid, including providing mitigation recommendations;

(E) conduct research on hardening solutions for critical components of the electric grid;

(F) conduct research on mitigation and recovery solutions for critical components of the electric grid; and

(G) provide technical assistance to States and other entities for standards and risk analysis.

(4) Savings provision

Nothing in this section authorizes new regulatory requirements.

(5) Authorization of appropriations

There is authorized to be appropriated to the Secretary to carry out this subsection $50,000,000 for the period of fiscal years 2022 through 2026.

(Pub. L. 117–58, div. D, title I, § 40125, Nov. 15, 2021, 135 Stat. 954.)

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.

§ 18725. Cybersecurity plan

(a) In general

The Secretary may require, as the Secretary determines appropriate, a recipient of any award or other funding under this division—

(1) to submit to the Secretary, prior to the issuance of the award or other funding, a cybersecurity plan that demonstrates the cybersecurity maturity of the recipient in the context of the project for which that award or other funding was provided; and

(2) establish a plan for maintaining and improving cybersecurity throughout the life of the proposed solution of the project.

(b) Contents of cybersecurity plan

A cybersecurity plan described in subsection (a) shall, at a minimum, describe how the recipient described in that subsection—

(1) plans to maintain cybersecurity between networks, systems, devices, applications, or components—

(A) within the proposed solution of the project; and

(B) at the necessary external interfaces at the proposed solution boundaries;

(2) will perform ongoing evaluation of cybersecurity risks to address issues as the issues arise throughout the life of the proposed solution;

(3) will report known or suspected network or system compromises of the project to the Secretary; and

(4) will leverage applicable cybersecurity programs of the Department, including cyber vulnerability testing and security engineering evaluations.

(c) Additional guidance

Each recipient described in subsection (a) should—

(1) maximize the use of open guidance and standards, including, wherever possible—

(A) the Cybersecurity Capability Maturity Model of the Department (or a successor model); and

(B) the Framework for Improving Critical Infrastructure Cybersecurity of the National Institute of Standards and Technology; and

(2) document—

(A) any deviation from open standards; and

(B) the utilization of proprietary standards where the recipient determines that such deviation necessary.

(d) Coordination

The Office of Cybersecurity, Energy Security, and Emergency Response of the Department shall review each cybersecurity plan submitted under subsection (a) to ensure integration with Department research, development, and demonstration programs.

(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.