(ii) were approved;

(iii) submitted security vulnerabilities; and

(iv) received compensation;

(B) the number and severity of all security vulnerabilities reported as part of such program;

(C) the number of previously unidentified security vulnerabilities remediated as a result of such program;

(D) the current number of outstanding previously unidentified security vulnerabilities and Department remediation plans for such outstanding vulnerabilities;

(E) the average length of time between the reporting of security vulnerabilities and remediation of such vulnerabilities;

(F) the types of compensation provided under such program;

(G) the lessons learned from such program;

(H) the public accessibility of contact information for the Department regarding the bug bounty program;

(I) the incorporation of bug bounty program identified vulnerabilities into existing Department vulnerability prioritization and management processes; and

(J) any challenges in implementing the bug bounty program and plans for expansion or contraction in the scope of the bug bounty program across Department information systems.

(Pub. L. 117–263, div. I, title XCV, § 9509, Dec. 23, 2022, 136 Stat. 3907.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

''Department'' and ''Secretary'' as used in this section mean the Department and Secretary of State, unless otherwise specified, see section 9002 of Pub. L. 117–263, set out as a note under section 2651 of this title.

§ 10307. Digital Connectivity and Cybersecurity Partnership

(a) Digital Connectivity and Cybersecurity Partnership

The Secretary is authorized to establish a program, which may be known as the ''Digital Connectivity and Cybersecurity Partnership'', to help foreign countries—

(1) expand and increase secure internet access and digital infrastructure in emerging markets, including demand for and availability of high-quality information and communications technology (ICT) equipment, software, and services;

(2) protect technological assets, including data;

(3) adopt policies and regulatory positions that foster and encourage open, interoperable, reliable, and secure internet, the free flow of data, multi-stakeholder models of internet governance, and pro-competitive and secure ICT policies and regulations;

(4) access United States exports of ICT goods and services;

(5) expand interoperability and promote the diversification of ICT goods and supply chain services to be less reliant on imports from the People's Republic of China;

(6) promote best practices and common standards for a national approach to cybersecurity; and

(7) advance other priorities consistent with paragraphs (1) through (6), as determined by the Secretary.

(b) Use of funds

Funds made available to carry out this section may be used to strengthen civilian cybersecurity and information and communications technology capacity, including participation of foreign law enforcement and military personnel in non-military activities, notwithstanding any other provision of law, provided that such support is essential to enabling civilian and law enforcement of cybersecurity and information and communication technology related activities in their respective countries.

(c) Implementation plan

Not later than 180 days after December 22, 2023, the Secretary shall submit to the appropriate congressional committees, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Oversight and Accountability of the House of Representatives an implementation plan for the coming year to advance the goals identified in subsection (a).

(d) Consultation

In developing and operationalizing the implementation plan required under subsection (c), the Secretary shall consult with—

(1) the appropriate congressional committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives;

(2) United States industry leaders;

(3) other relevant technology experts, including the Open Technology Fund;

(4) representatives from relevant United States Government agencies; and

(5) representatives from like-minded allies and partners.

(e) Authorization of appropriations

For the purposes of carrying out this section, funds authorized to be appropriated to carry out chapter 4 of part II of the Foreign Assistance Act of 1961 (22 U.S.C. 2346 et seq.) may be made available, notwithstanding any other provision of law to strengthen civilian cybersecurity and information and communications technology capacity, including for participation of foreign law enforcement and military personnel in non-military activities, and for contributions to international organizations and international financial institutions of which the United States is a member. Such funds shall remain available until expended.

(Pub. L. 118–31, div. F, title LXIII, § 6306, Dec. 22, 2023, 137 Stat. 989.)

Editorial Notes

REFERENCES IN TEXT

The Foreign Assistance Act of 1961, referred to in subsec. (e), is Pub. L. 87–195, Sept. 4, 1961, 75 Stat. 424. Chapter 4 of part II of the Act is classified generally to part IV (§ 2346 et seq.) of subchapter II of chapter 32 of

this title. For complete classification of this Act to the Code, see Short Title note set out under section 2151 of this title and Tables.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of ''Secretary'' and ''appropriate congressional committees'' as used in this section, see section 6002 of Pub. L. 118–31, set out as a note under section 2651 of this title.

§ 10308. Cyber protection support for personnel of the Department of State in positions highly vulnerable to cyber attack

(a) Definitions

In this section:

(1) At-risk personnel

The term ''at-risk personnel'' means personnel of the Department—

(A) whom the Secretary determines to be highly vulnerable to cyber attacks and hostile information collection activities because of their positions in the Department; and

(B) whose personal technology devices or personal accounts are highly vulnerable to cyber attacks and hostile information collection activities.

(2) Personal accounts

The term ''personal accounts'' means accounts for online and telecommunications services, including telephone, residential internet access, email, text and multimedia messaging, cloud computing, social media, health care, and financial services, used by Department personnel outside of the scope of their employment with the Department.

(3) Personal technology devices

The term ''personal technology devices'' means technology devices used by personnel of the Department outside of the scope of their employment with the Department, including networks to which such devices connect.

(b) Requirement to provide cyber protection support

The Secretary, in consultation with the Secretary of Homeland Security and the Director of National Intelligence, as appropriate—

(1) shall offer cyber protection support for the personal technology devices and personal accounts of at-risk personnel; and

(2) may provide the support described in paragraph (1) to any Department personnel who request such support.

(c) Nature of cyber protection support

Subject to the availability of resources, the cyber protection support provided to personnel pursuant to subsection (b) may include training, advice, assistance, and other services relating to protection against cyber attacks and hostile information collection activities.

(d) Privacy protections for personal devices

The Department is prohibited pursuant to this section from accessing or retrieving any information from any personal technology device or personal account of Department employees unless—

(1) access or information retrieval is necessary for carrying out the cyber protection support specified in this section; and

(2) the Department has received explicit consent from the employee to access a personal technology device or personal account prior to each time such device or account is accessed.

(e) Rule of construction

Nothing in this section may be construed—

(1) to encourage Department personnel to use personal technology devices for official business; or

(2) to authorize cyber protection support for senior Department personnel using personal devices, networks, and personal accounts in an official capacity.

(f) Report

(1) In general

Not later than 180 days after December 22, 2023, the Secretary shall submit to the appropriate committees of Congress a report regarding the provision of cyber protection support pursuant to subsection (b), which shall include—

(A) a description of the methodology used to make the determination under subsection (a)(1); and

(B) guidance for the use of cyber protection support and tracking of support requests for personnel receiving cyber protection support pursuant to subsection (b).

(2) Appropriate committees of Congress defined

In this subsection, the term ''appropriate committees of Congress'' means—

(A) the appropriate congressional committees;

(B) the Select Committee on Intelligence and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Permanent Select Committee on Intelligence and the Committee on Oversight and Accountability of the House of Representatives.

(Pub. L. 118–31, div. F, title LXIII, § 6308, Dec. 22, 2023, 137 Stat. 993.)

Statutory Notes and Related Subsidiaries

MEASURES TO PROTECT DEPARTMENT DEVICES FROM THE PROLIFERATION AND USE OF FOREIGN COMMERCIAL SPYWARE

Pub. L. 118–159, div. G, title LXXIII, § 7302, Dec. 23, 2024, 138 Stat. 2541, provided that:

''(a) DEFINITIONS.—In this section:

''(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term 'appropriate committees of Congress' means—

''(A) the Committee on Foreign Relations, the Select Committee on Intelligence, the Committee on Homeland Security and Governmental Affairs, and the Committee on Armed Services of the Senate; and

''(B) the Committee on Foreign Affairs, the Permanent Select Committee on Intelligence, the Committee on Homeland Security, and the Committee on Armed Services of the House of Representatives.

''(2) COVERED DEVICE.—The term 'covered device' means any electronic mobile device, including smartphones, tablet computing devices, or laptop