(4) assigning not fewer than 2 Regional Technology Officers to posts within—

(A) each regional bureau of the Department; and

(B) the Bureau of International Organization Affairs.

(c) Annual briefing requirement

Not later than 180 days after December 23, 2022, and annually thereafter for the following 5 years, the Secretary shall brief the appropriate congressional committees regarding the status of the implementation plan required under subsection (b).

(d) Authorization of appropriations

There is authorized to be appropriated up to $25,000,000 for each of the fiscal years 2023 through 2027 to carry out this section.

(Pub. L. 117–263, div. I, title XCV, § 9508, Dec. 23, 2022, 136 Stat. 3906; Pub. L. 118–159, div. G, title LXXIII, § 7301, Dec. 23, 2024, 138 Stat. 2541.)

Editorial Notes

AMENDMENTS

2024—Subsec. (a)(1). Pub. L. 118–159 inserted '', and shall be administered by the Bureau for Cyberspace and Digital Policy'' before period at end.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of ''Secretary'', ''appropriate congressional committees'', and ''Department'' as used in this section, see section 9002 of Pub. L. 117–263, set out as a note under section 2651 of this title.

§ 10306. Vulnerability disclosure policy and bug bounty program report

(a) Definitions

In this section:

(1) Bug bounty program

The term ''bug bounty program'' means a program under which an approved individual, organization, or company is temporarily authorized to identify and report vulnerabilities of internet-facing information technology of the Department in exchange for compensation.

(2) Information technology

The term ''information technology'' has the meaning given such term in section 11101 of title 40.

(b) Vulnerability Disclosure Policy

(1) In general

Not later than 180 days after December 23, 2022, the Secretary shall design, establish, and make publicly known a Vulnerability Disclosure Policy (referred to in this section as the ''VDP'') to improve Department cybersecurity by—

(A) creating Department policy and infrastructure to receive reports of and remediate discovered vulnerabilities in line with existing policies of the Office of Management and Budget and the Department of Homeland Security Binding Operational Directive 20–01 or any subsequent directive; and

(B) providing a report on such policy and infrastructure to Congress.

(2) Annual reports

Not later than 180 days after the establishment of the VDP pursuant to paragraph (1), and annually thereafter for the following 5 years, the Secretary shall submit a report on the VDP to the Committee on Foreign Relations of the Senate, the Committee on Homeland Security and Governmental Affairs of the Senate, the Select Committee on Intelligence of the Senate, the Committee on Foreign Affairs of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Permanent Select Committee on Intelligence of the House of Representatives that includes information relating to—

(A) the number and severity of all security vulnerabilities reported;

(B) the number of previously unidentified security vulnerabilities remediated as a result;

(C) the current number of outstanding previously unidentified security vulnerabilities and Department of State remediation plans;

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

(E) the resources, surge staffing, roles, and responsibilities within the Department used to implement the VDP and complete security vulnerability remediation;

(F) how the VDP identified vulnerabilities are incorporated into existing Department vulnerability prioritization and management processes;

(G) any challenges in implementing the VDP and plans for expansion or contraction in the scope of the VDP across Department information systems; and

(H) any other topic that the Secretary determines to be relevant.

(c) Bug bounty program report

(1) In general

Not later than 180 days after December 23, 2022, the Secretary shall submit a report to Congress that describes any ongoing efforts by the Department or a third-party vendor under contract with the Department to establish or carry out a bug bounty program that identifies security vulnerabilities of internet-facing information technology of the Department.

(2) Report

Not later than 180 days after the date on which any bug bounty program is established, the Secretary shall submit a report to the Committee on Foreign Relations of the Senate, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Homeland Security of the House of Representatives regarding such program, including information relating to—

(A) the number of approved individuals, organizations, or companies involved in such program, disaggregated by the number of approved individuals, organizations, or companies that—

(i) registered;

(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