

emerging technology, and technology and digital policy;

(2) a list of which hiring authorities described in paragraph (1) have been used during the previous 5 years;

(3) the number of employees in qualified positions hired, aggregated by position and grade level or pay band;

(4) the number of employees who have been placed in qualified positions, aggregated by bureau and offices within the Department;

(5) the rate of attrition of individuals who begin the hiring process and do not complete the process and a description of the reasons for such attrition;

(6) the number of individuals who are interviewed by subject matter experts and the number of individuals who are not interviewed by subject matter experts; and

(7) recommendations for—

(A) reducing the attrition rate referred to in paragraph (5) by 5 percent each year;

(B) additional hiring authorities needed to acquire needed technology talent;

(C) hiring personnel to hold public trust positions until such personnel can obtain the necessary security clearance; and

(D) informing and training supervisors within the Department on the use of the authorities listed in paragraph (1).

**(d) Incentive pay for cybersecurity professionals**

To increase the number of qualified candidates available to fulfill the cybersecurity needs of the Department, the Secretary shall—

(1) include computer programming languages within the Recruitment Language Program; and

(2) provide appropriate language incentive pay.

**(e) Report**

Not later than 1 year after December 23, 2022, and annually thereafter for the following 5 years, the Secretary shall provide a list to the appropriate congressional committees that identifies—

(1) the computer programming languages included within the Recruitment Language Program and the language incentive pay rate; and

(2) the number of individuals benefitting from the inclusion of such computer programming languages in the Recruitment Language Program and language incentive pay.

(Pub. L. 117–263, div. I, title XCV, §9506, Dec. 23, 2022, 136 Stat. 3904.)

**Statutory Notes and Related Subsidiaries**

DEFINITIONS

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

**§ 10304. Short course on emerging technologies for senior officials**

**(a) In general**

Not later than 1 year after December 23, 2022, the Secretary shall develop and begin providing, for senior officials of the Department, a course

addressing how the most recent and relevant technologies affect the activities of the Department.

**(b) Throughput objectives**

The Secretary should ensure that—

(1) during the first year that the course developed pursuant to subsection (a) is offered, not fewer than 20 percent of senior officials are certified as having passed such course; and

(2) in each subsequent year, until the date on which 80 percent of senior officials are certified as having passed such course, an additional 10 percent of senior officials are certified as having passed such course.

(Pub. L. 117–263, div. I, title XCV, §9507, Dec. 23, 2022, 136 Stat. 3906.)

**Statutory Notes and Related Subsidiaries**

DEFINITIONS

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

**§ 10305. Establishment and expansion of Regional Technology Officer Program**

**(a) Regional Technology Officer Program**

**(1) Establishment**

The Secretary shall establish a program, which shall be known as the “Regional Technology Officer Program” (referred to in this section as the “Program”), and shall be administered by the Bureau for Cyberspace and Digital Policy.

**(2) Goals**

The goals of the Program shall include the following:

(A) Promoting United States leadership in technology abroad.

(B) Working with partners to increase the deployment of critical and emerging technology in support of democratic values.

(C) Shaping diplomatic agreements in regional and international fora with respect to critical and emerging technologies.

(D) Building diplomatic capacity for handling critical and emerging technology issues.

(E) Facilitating the role of critical and emerging technology in advancing the foreign policy objectives of the United States through engagement with research labs, incubators, and venture capitalists.

(F) Maintaining the advantages of the United States with respect to critical and emerging technologies.

**(b) Implementation plan**

Not later than 180 days after December 23, 2022, the Secretary shall submit an implementation plan to the appropriate congressional committees that outlines strategies for—

(1) advancing the goals described in subsection (a)(2);

(2) hiring Regional Technology Officers and increasing the competitiveness of the Program within the Foreign Service bidding process;

(3) expanding the Program to include a minimum of 15 Regional Technology Officers; and

(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;