§ 663. Federal intrusion detection and prevention system

(a) Definitions

In this section—

(1) the term ''agency'' has the meaning given the term in section 3502 of title 44;

(2) the term ''agency information'' means information collected or maintained by or on behalf of an agency;[1]

(3) the term ''agency information system'' has the meaning given the term in section 660 of this title; and[2]

(b) Requirement

(1) In general

Not later than 1 year after December 18, 2015, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

(2) Regular improvement

The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

(c) Activities

In carrying out subsection (b), the Secretary—

(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy, operate, and maintain technologies in accordance with subsection (b);

(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and noncommercial technologies and detection technologies beyond signature-based detection, and acquire, test, and deploy such technologies when appropriate;

(5) shall establish a pilot through which the Secretary may acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4); and

(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note).

(d) Principles

In carrying out subsection (b), the Secretary shall ensure that—

(1) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(2) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(3) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

(4) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

(e) Private entities

(1) Conditions

A private entity described in subsection (c)(2) may not—

(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity other than the Department or the agency that disclosed the information under subsection (c)(1), including personal information of a specific individual or information that identifies a specific individual not directly related to a cybersecurity risk; or

(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

(2) Limitation on liability

No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

(3) Rule of construction

Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

[1] So in original. Probably should be followed by ''and''.

[2] So in original. The ''; and'' probably should be a period.

(f) Privacy Officer review

Not later than 1 year after December 18, 2015, the Privacy Officer appointed under section 142 of this title, in consultation with the Attorney General, shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable privacy laws, including those governing the acquisition, interception, retention, use, and disclosure of communications.

(Pub. L. 107–296, title XXII, § 2213, formerly title II, § 230, as added Pub. L. 114–113, div. N, title II, § 223(a)(6), Dec. 18, 2015, 129 Stat. 2964; renumbered title XXII, § 2213, and amended Pub. L. 115–278, § 2(g)(2)(I), (9)(A)(vii), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(H), Dec. 23, 2022, 136 Stat. 3660.)

Editorial Notes

REFERENCES IN TEXT

Section 208(b) of the E-Government Act of 2002, referred to in subsec. (c)(6), is section 208(b) of title II of Pub. L. 107–347, which is set out in a note under section 3501 of Title 44, Public Printing and Documents.

CODIFICATION

Section was formerly classified to section 151 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2022—Subsec. (a)(4). Pub. L. 117–263 struck out par. (4) which read as follows: ''the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 659 of this title.''

2018—Subsec. (a)(3). Pub. L. 115–278, § 2(g)(9)(A)(vii)(I), substituted ''section 660 of this title'' for ''section 149 of this title''.

Subsec. (a)(4). Pub. L. 115–278, § 2(g)(9)(A)(vii)(II), substituted ''section 659 of this title'' for ''section 148 of this title''.

Statutory Notes and Related Subsidiaries

COMPETITION RELATING TO CYBERSECURITY VULNERABILITIES

Pub. L. 117–81, div. A, title XV, § 1544, Dec. 27, 2021, 135 Stat. 2057, provided that: ''The Under Secretary for Science and Technology of the Department of Homeland Security, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department, may establish an incentive-based program that allows industry, individuals, academia, and others to compete in identifying remediation solutions for cybersecurity vulnerabilities (as such term is defined in section 2209 of the Homeland Security Act of 2002 [6 U.S.C. 659]) to information systems (as such term is defined in such section 2209 [see 6 U.S.C. 650]) and industrial control systems, including supervisory control and data acquisition systems.''

DEPARTMENT OF HOMELAND SECURITY DISCLOSURE OF SECURITY VULNERABILITIES

Pub. L. 115–390, title I, § 101, Dec. 21, 2018, 132 Stat. 5173, provided that:

''(a) VULNERABILITY DISCLOSURE POLICY.—The Secretary of Homeland Security shall establish a policy applicable to individuals, organizations, and companies that report security vulnerabilities on appropriate information systems of Department of Homeland Security. Such policy shall include each of the following:

''(1) The appropriate information systems of the Department that individuals, organizations, and companies may use to discover and report security vulnerabilities on appropriate information systems.

''(2) The conditions and criteria under which individuals, organizations, and companies may operate to discover and report security vulnerabilities.

''(3) How individuals, organizations, and companies may disclose to the Department security vulnerabilities discovered on appropriate information systems of the Department.

''(4) The ways in which the Department may communicate with individuals, organizations, and companies that report security vulnerabilities.

''(5) The process the Department shall use for public disclosure of reported security vulnerabilities.

''(b) REMEDIATION PROCESS.—The Secretary of Homeland Security shall develop a process for the Department of Homeland Security to address the mitigation or remediation of the security vulnerabilities reported through the policy developed in subsection (a).

''(c) CONSULTATION.—

''(1) IN GENERAL.—In developing the security vulnerability disclosure policy under subsection (a), the Secretary of Homeland Security shall consult with each of the following:

''(A) The Attorney General regarding how to ensure that individuals, organizations, and companies that comply with the requirements of the policy developed under subsection (a) are protected from prosecution under section 1030 of title 18, United States Code, civil lawsuits, and similar provisions of law with respect to specific activities authorized under the policy.

''(B) The Secretary of Defense and the Administrator of General Services regarding lessons that may be applied from existing vulnerability disclosure policies.

''(C) Non-governmental security researchers.

''(2) NONAPPLICABILITY OF FACA.—The Federal Advisory Committee Act ([former] 5 U.S.C. App.) [see 5 U.S.C. 1001 et seq.] shall not apply to any consultation under this section.

''(d) PUBLIC AVAILABILITY.—The Secretary of Homeland Security shall make the policy developed under subsection (a) publicly available.

''(e) SUBMISSION TO CONGRESS.—

''(1) DISCLOSURE POLICY AND REMEDIATION PROCESS.—Not later than 90 days after the date of the enactment of this Act [Dec. 21, 2018], the Secretary of Homeland Security shall submit to the appropriate congressional committees a copy of the policy required under subsection (a) and the remediation process required under subsection (b).

''(2) REPORT AND BRIEFING.—

''(A) REPORT.—Not later than one year after establishing the policy required under subsection (a), the Secretary of Homeland Security shall submit to the appropriate congressional committees a report on such policy and the remediation process required under subsection (b).

''(B) ANNUAL BRIEFINGS.—One year after the date of the submission of the report under subparagraph (A), and annually thereafter for each of the next three years, the Secretary of Homeland Security shall provide to the appropriate congressional committees a briefing on the policy required under subsection (a) and the process required under subsection (b).

''(C) MATTERS FOR INCLUSION.—The report required under subparagraph (A) and the briefings required under subparagraph (B) shall include each of the following with respect to the policy required under subsection (a) and the process required under subsection (b) for the period covered by the report or briefing, as the case may be:

''(i) The number of unique security vulnerabilities reported.

''(ii) The number of previously unknown security vulnerabilities mitigated or remediated.

''(iii) The number of unique individuals, organizations, and companies that reported security vulnerabilities.

''(iv) The average length of time between the reporting of security vulnerabilities and mitigation or remediation of such vulnerabilities.

''(f) DEFINITIONS.—In this section:

''(1) The term 'security vulnerability' has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17)), in information technology.

''(2) The term 'information system' has the meaning given that term by section 3502 of title 44, United States Code.

''(3) The term 'appropriate information system' means an information system that the Secretary of Homeland Security selects for inclusion under the vulnerability disclosure policy required by subsection (a).

''(4) The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security, the Committee on Armed Services, the Committee on Energy and Commerce, and the Permanent Select Committee on Intelligence of the House of Representatives; and

''(B) the Committee on Homeland Security and Governmental Affairs, the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, and the Select Committee on Intelligence of the Senate.''

DEPARTMENT OF HOMELAND SECURITY BUG BOUNTY PILOT PROGRAM

Pub. L. 115–390, title I, § 102, Dec. 21, 2018, 132 Stat. 5175, provided that:

''(a) DEFINITIONS.—In this section:

''(1) The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(B) the Select Committee on Intelligence of the Senate;

''(C) the Committee on Homeland Security of the House of Representatives; and

''(D) Permanent Select Committee on Intelligence of the House of Representatives.

''(2) The term 'bug bounty program' means a program under which—

''(A) individuals, organizations, and companies are temporarily authorized to identify and report vulnerabilities of appropriate information systems of the Department; and

''(B) eligible individuals, organizations, and companies receive compensation in exchange for such reports.

''(3) The term 'Department' means the Department of Homeland Security.

''(4) The term 'eligible individual, organization, or company' means an individual, organization, or company that meets such criteria as the Secretary determines in order to receive compensation in compliance with Federal laws.

''(5) The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

''(6) The term 'pilot program' means the bug bounty pilot program required to be established under subsection (b)(1).

''(7) The term 'Secretary' means the Secretary of Homeland Security.

''(b) BUG BOUNTY PILOT PROGRAM.—

''(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this Act [Dec. 21, 2018], the Secretary shall establish, within the Office of the Chief Information Officer, a bug bounty pilot program to minimize vulnerabilities of appropriate information systems of the Department.

''(2) RESPONSIBILITIES OF SECRETARY.—In establishing and conducting the pilot program, the Secretary shall—

''(A) designate appropriate information systems to be included in the pilot program;

''(B) provide compensation to eligible individuals, organizations, and companies for reports of previously unidentified security vulnerabilities within the information systems designated under subparagraph (A);

''(C) establish criteria for individuals, organizations, and companies to be considered eligible for compensation under the pilot program in compliance with Federal laws;

''(D) consult with the Attorney General on how to ensure that approved individuals, organizations, or companies that comply with the requirements of the pilot program are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law, and civil lawsuits for specific activities authorized under the pilot program;

''(E) consult with the Secretary of Defense and the heads of other departments and agencies that have implemented programs to provide compensation for reports of previously undisclosed vulnerabilities in information systems, regarding lessons that may be applied from such programs; and

''(F) develop an expeditious process by which an individual, organization, or company can register with the Department, submit to a background check as determined by the Department, and receive a determination as to eligibility; and

''(G) engage qualified interested persons, including non-government sector representatives, about the structure of the pilot program as constructive and to the extent practicable.

''(3) CONTRACT AUTHORITY.—In establishing the pilot program, the Secretary, subject to the availability of appropriations, may award 1 or more competitive contracts to an entity, as necessary, to manage the pilot program.

''(c) REPORT TO CONGRESS.—Not later than 180 days after the date on which the pilot program is completed, the Secretary shall submit to the appropriate congressional committees a report on the pilot program, which shall include—

''(1) the number of individuals, organizations, or companies that participated in the pilot program, broken down by the number of individuals, organizations, or companies that—

''(A) registered;

''(B) were determined eligible;

''(C) submitted security vulnerabilities; and

''(D) received compensation;

''(2) the number and severity of vulnerabilities reported as part of the pilot program;

''(3) the number of previously unidentified security vulnerabilities remediated as a result of the pilot program;

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

''(5) the average length of time between the reporting of security vulnerabilities and remediation of the vulnerabilities;

''(6) the types of compensation provided under the pilot program; and

''(7) the lessons learned from the pilot program.

''(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Department $250,000 for fiscal year 2019 to carry out this section.''

AGENCY RESPONSIBILITIES

Pub. L. 114–113, div. N, title II, § 223(b), Dec. 18, 2015, 129 Stat. 2966, as amended by Pub. L. 115–278, § 2(h)(1)(E), Nov. 16, 2018, 132 Stat. 4182, provided that:

''(1) IN GENERAL.—Except as provided in paragraph (2)—

''(A) not later than 1 year after the date of enactment of this Act [Dec. 18, 2015] or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under section 2213(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)(1)], whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an

agency information system and any information system other than an agency information system; and

''(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to section 2213(b)(2) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)(2)], the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

''(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

''(3) DEFINITION.—Notwithstanding section 222 [6 U.S.C. 1521], in this subsection, the term 'agency information system' means an information system owned or operated by an agency.

''(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit an agency from applying the intrusion detection and prevention capabilities to an information system other than an agency information system under section 2213(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)(1)], at the discretion of the head of the agency or as provided in relevant policies, directives, and guidelines.''

§ 664. National asset database

(a) Establishment

(1) National asset database

The Secretary shall establish and maintain a national database of each system or asset that—

(A) the Secretary, in consultation with appropriate homeland security officials of the States, determines to be vital and the loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States, any State, or any local government; or

(B) the Secretary determines is appropriate for inclusion in the database.

(2) Prioritized critical infrastructure list

In accordance with Homeland Security Presidential Directive–7, as in effect on January 1, 2007, the Secretary shall establish and maintain a single classified prioritized list of systems and assets included in the database under paragraph (1) that the Secretary determines would, if destroyed or disrupted, cause national or regional catastrophic effects.

(b) Use of database

The Secretary shall use the database established under subsection (a)(1) in the development and implementation of Department plans and programs as appropriate.

(c) Maintenance of database

(1) In general

The Secretary shall maintain and annually update the database established under subsection (a)(1) and the list established under subsection (a)(2), including—

(A) establishing data collection guidelines and providing such guidelines to the appropriate homeland security official of each State;

(B) regularly reviewing the guidelines established under subparagraph (A), including by consulting with the appropriate homeland security officials of States, to solicit feedback about the guidelines, as appropriate;

(C) after providing the homeland security official of a State with the guidelines under subparagraph (A), allowing the official a reasonable amount of time to submit to the Secretary any data submissions recommended by the official for inclusion in the database established under subsection (a)(1);

(D) examining the contents and identifying any submissions made by such an official that are described incorrectly or that do not meet the guidelines established under subparagraph (A); and

(E) providing to the appropriate homeland security official of each relevant State a list of submissions identified under subparagraph (D) for review and possible correction before the Secretary finalizes the decision of which submissions will be included in the database established under subsection (a)(1).

(2) Organization of information in database

The Secretary shall organize the contents of the database established under subsection (a)(1) and the list established under subsection (a)(2) as the Secretary determines is appropriate. Any organizational structure of such contents shall include the categorization of the contents—

(A) according to the sectors listed in National Infrastructure Protection Plan developed pursuant to Homeland Security Presidential Directive–7; and

(B) by the State and county of their location.

(3) Private sector integration

The Secretary shall identify and evaluate methods, including the Department's Protected Critical Infrastructure Information Program, to acquire relevant private sector information for the purpose of using that information to generate any database or list, including the database established under subsection (a)(1) and the list established under subsection (a)(2).

(4) Retention of classification

The classification of information required to be provided to Congress, the Department, or any other department or agency under this section by a Sector Risk Management Agency, including the assignment of a level of classification of such information, shall be binding on Congress, the Department, and that other Federal agency.

(d) Reports

(1) Report required

Not later than 180 days after August 3, 2007, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the database established under subsection (a)(1) and the list established under subsection (a)(2).

(2) Contents of report

Each such report shall include the following: