(b) Contents

The strategy required under subsection (a) shall include the following:

(1) Strategic and operational goals and priorities to successfully execute the full range of the Secretary's cybersecurity responsibilities.

(2) Information on the programs, policies, and activities that are required to successfully execute the full range of the Secretary's cybersecurity responsibilities, including programs, policies, and activities in furtherance of the following:

(A) Cybersecurity functions set forth in section 659 of this title (relating to the national cybersecurity and communications integration center).

(B) Cybersecurity investigations capabilities.

(C) Cybersecurity research and development.

(D) Engagement with international cybersecurity partners.

(c) Considerations

In developing the strategy required under subsection (a), the Secretary shall—

(1) consider—

(A) the cybersecurity strategy for the Homeland Security Enterprise published by the Secretary in November 2011;

(B) the Department of Homeland Security Fiscal Years 2014–2018 Strategic Plan; and

(C) the most recent Quadrennial Homeland Security Review issued pursuant to section 347 of this title; and

(2) include information on the roles and responsibilities of components and offices of the Department, to the extent practicable, to carry out such strategy.

(d) Implementation plan

Not later than 90 days after the development of the strategy required under subsection (a), the Secretary shall issue an implementation plan for the strategy that includes the following:

(1) Strategic objectives and corresponding tasks.

(2) Projected timelines and costs for such tasks.

(3) Metrics to evaluate performance of such tasks.

(e) Congressional oversight

The Secretary shall submit to Congress for assessment the following:

(1) A copy of the strategy required under subsection (a) upon issuance.

(2) A copy of the implementation plan required under subsection (d) upon issuance, together with detailed information on any associated legislative or budgetary proposals.

(f) Classified information

The strategy required under subsection (a) shall be in an unclassified form but may contain a classified annex.

(g) Rule of construction

Nothing in this section may be construed as permitting the Department to engage in monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual's personally identifiable information.

(Pub. L. 107–296, title XXII, §2211, formerly title II, §228A, as added Pub. L. 114–328, div. A, title XIX, §1912(a), Dec. 23, 2016, 130 Stat. 2683; renumbered title XXII, §2211, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(v), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(F), Dec. 23, 2022, 136 Stat. 3660.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 149a of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2022—Subsec. (h). Pub. L. 117–263 struck out subsec. (h). Text read as follows: ''In this section, the term 'Homeland Security Enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts.''

2018—Subsec. (b)(2)(A). Pub. L. 115–278, §2(g)(9)(A)(v), substituted ''section 659 of this title'' for ''the section 148 of this title''.

§ 662. Clearances

The Secretary shall make available the process of application for security clearances under Executive Order 13549 (75 Fed. Reg. 162;[1] relating to a classified national security information program) or any successor Executive Order to appropriate representatives of sector coordinating councils, sector Information Sharing and Analysis Organizations, owners and operators of critical infrastructure, and any other person that the Secretary determines appropriate.

(Pub. L. 107–296, title XXII, §2212, formerly title II, §229, formerly §228, as added Pub. L. 113–282, §7(a), Dec. 18, 2014, 128 Stat. 3070; renumbered §229, Pub. L. 114–113, div. N, title II, §223(a)(1), Dec. 18, 2015, 129 Stat. 2963; renumbered title XXII, §2212, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(vi), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(G), Dec. 23, 2022, 136 Stat. 3660.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 13549, referred to in text, is Ex. Ord. No. 13549, Aug. 18, 2010, 75 F.R. 51609, which is set out as a note under section 3161 of Title 50, War and National Defense.

CODIFICATION

Section was formerly classified to section 150 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2022—Pub. L. 117–263 substituted ''Information Sharing and Analysis Organizations'' for ''information sharing and analysis organizations (as defined in section 671(5) of this title)''.

2018—Pub. L. 115–278, §2(g)(9)(A)(vi), substituted ''section 671(5) of this title'' for ''section 131(5) of this title''.

[1] So in original. Probably should be ''51609;''.

§ 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.