(3) the term ''intelligence community'' has the meaning given the term in section 3003(4) of title 50; and

(4) the term ''national security system'' has the meaning given the term in section 11103 of title 40.

(b) Intrusion assessment plan

(1) Requirement

The Secretary, in coordination with the Director of the Office of Management and Budget, shall—

(A) develop and implement an intrusion assessment plan to proactively detect, identify, and remove intruders in agency information systems on a routine basis; and

(B) update such plan as necessary.

(2) Exception

The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(c) Cyber incident response plan

The Under Secretary appointed under section 113(a)(1)(H) of this title shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 131(5) of this title), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 148 of this title) to critical infrastructure.

(d) National Response Framework

The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (c), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

(Pub. L. 107–296, title II, § 228, as added and amended Pub. L. 114–113, div. N, title II, §§ 205, 223(a)(2), (4), (5), Dec. 18, 2015, 129 Stat. 2961, 2963, 2964.)

CODIFICATION

Former section 149 of this title, which was transferred and redesignated as subsec. (c) of this section by Pub. L. 114–113, div. N, title II, § 223(a)(2), Dec. 18, 2015, 129 Stat. 2963, was based on Pub. L. 107–296, title II, § 227, as added by Pub. L. 113–282, § 7(a), Dec. 18, 2014, 128 Stat. 3070.

PRIOR PROVISIONS

A prior section 228 of Pub. L. 107–296 was renumbered section 229 and is classified to section 150 of this title.

AMENDMENTS

2015—Subsec. (c). Pub. L. 114–113, § 223(a)(5), made technical amendment to reference in original act which appears in text as reference to section 148 of this title.

Pub. L. 114–113, § 223(a)(2), transferred former section 149 of this title to subsec. (c) of this section. See Codification note above.

Subsec. (d). Pub. L. 114–113, § 205, added subsec. (d).

RULE OF CONSTRUCTION

Pub. L. 113–282, § 7(c), Dec. 18, 2014, 128 Stat. 3072, provided that: ''Nothing in the amendment made by subsection (a) [enacting subsec. (c) of this section and section 150 of this title] or in subsection (b)(1) [formerly classified as a note under section 3543 of Title 44, Public Printing and Documents, see now section 2(d)(1) of Pub. L. 113–283, set out as a note under section 3553 of Title 44] shall be construed to alter any authority of a Federal agency or department.''

§ 149a. Cybersecurity strategy

(a) In general

Not later than 90 days after December 23, 2016, the Secretary shall develop a departmental strategy to carry out cybersecurity responsibilities as set forth in law.

(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 the[1] section 148 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.

[1] So in original.

(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.

(h) Definition

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.

(Pub. L. 107–296, title II, § 228A, as added Pub. L. 114–328, div. A, title XIX, § 1912(a), Dec. 23, 2016, 130 Stat. 2683.)

§ 150. 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 (as defined in section 131(5) of this title), owners and operators of critical infrastructure, and any other person that the Secretary determines appropriate.

(Pub. L. 107–296, 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.)

REFERENCES IN TEXT

Executive Order 13549, referred to in text, is set out as a note under section 3161 of Title 50, War and National Defense.

§ 151. 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;

(3) the term ''agency information system'' has the meaning given the term in section 149 of this title; and

(4) the terms ''cybersecurity risk'' and ''information system'' have the meanings given those terms in section 148 of this title.

(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).

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