

Subsec. (e)(1)(A). Pub. L. 114–113, §203(4)(A)(i), inserted “cyber threat indicators, defensive measures, and” before “information”.

Subsec. (e)(1)(B). Pub. L. 114–113, §203(4)(A)(ii), inserted “cyber threat indicators, defensive measures, and” before “information related”.

Subsec. (e)(1)(F). Pub. L. 114–113, §203(4)(A)(iii), substituted “cyber threat indicators, defensive measures, cybersecurity risks,” for “cybersecurity risks” and struck out “and” at end.

Subsec. (e)(1)(G). Pub. L. 114–113, §203(4)(A)(iv), substituted “cyber threat indicators, defensive measures, cybersecurity risks, and incidents; and” for “cybersecurity risks and incidents”.

Subsec. (e)(1)(H). Pub. L. 114–113, §203(4)(A)(v), added subpar. (H).

Subsec. (e)(2). Pub. L. 114–113, §203(4)(B), substituted “cyber threat indicators, defensive measures, cybersecurity risks,” for “cybersecurity risks” and inserted “or disclosure” after “access”.

Subsec. (e)(3). Pub. L. 114–113, §203(4)(C), inserted “, including by working with the Privacy Officer appointed under section 142 of this title to ensure that the Center follows the policies and procedures specified in subsections (b) and (d)(5)(C) of section 105 of the Cybersecurity Act of 2015” before period at end.

Subsecs. (g) to (l). Pub. L. 114–113, §203(5), added subsecs. (g) to (l).

RULES OF CONSTRUCTION

Pub. L. 113–282, §8, Dec. 18, 2014, 128 Stat. 3072, provided that:

“(a) PROHIBITION ON NEW REGULATORY AUTHORITY.—Nothing in this Act [see section 1 of Pub. L. 113–282, set out as a Short Title of 2014 Amendment note under section 101 of this title] or the amendments made by this Act shall be construed to grant the Secretary [of Homeland Security] any authority to promulgate regulations or set standards relating to the cybersecurity of private sector critical infrastructure that was not in effect on the day before the date of enactment of this Act [Dec. 18, 2014].

“(b) PRIVATE ENTITIES.—Nothing in this Act or the amendments made by this Act shall be construed to require any private entity—

“(1) to request assistance from the Secretary; or

“(2) that requested such assistance from the Secretary to implement any measure or recommendation suggested by the Secretary.”

DEFINITIONS

Pub. L. 113–282, §2, Dec. 18, 2014, 128 Stat. 3066, provided that: “In this Act [see section 1 of Pub. L. 113–282, set out as a Short Title of 2014 Amendment note under section 101 of this title]—

“(1) the term ‘Center’ means the national cybersecurity and communications integration center under section 226 [renumbered 227 by section 223(a)(3) of Pub. L. 114–113 and renumbered 2209 by section 2(g)(2)(I) of Pub. L. 115–278] of the Homeland Security Act of 2002 [6 U.S.C. 659], as added by section 3;

“(2) the term ‘critical infrastructure’ has the meaning given that term in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101);

“(3) the term ‘cybersecurity risk’ has the meaning given that term in section 226 [2209] of the Homeland Security Act of 2002, as added by section 3;

“(4) the term ‘information sharing and analysis organization’ has the meaning given that term in section 212(5) [renumbered 222(5) by section 2(g)(2)(H) of Pub. L. 115–278] of the Homeland Security Act of 2002 [former] 6 U.S.C. 131(5) [now 6 U.S.C. 671(5)];

“(5) the term ‘information system’ has the meaning given that term in section 3502(8) of title 44, United States Code; and

“(6) the term ‘Secretary’ means the Secretary of Homeland Security.”

§ 660. Cybersecurity plans

(a) Definitions

In this section—

(1) the term “agency information system” means an information system used or operated by an agency or by another entity on behalf of an agency;

(2) the terms “cybersecurity risk” and “information system” have the meanings given those terms in section 659 of this title;

(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 Director of Cybersecurity and Infrastructure Security 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 671(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 659 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 XXII, §2210, formerly 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; renumbered title XXII, §2210, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(iv), Nov. 16, 2018, 132 Stat. 4178, 4181.)

CODIFICATION

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

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.

AMENDMENTS

2018—Subsec. (a)(2). Pub. L. 115–278, §2(g)(9)(A)(iv)(I), substituted “section 659 of this title” for “section 148 of this title”.

Subsec. (c). Pub. L. 115–278, §2(g)(9)(A)(iv), substituted “Director of Cybersecurity and Infrastructure Security” for “Under Secretary appointed under section 113(a)(1)(H) of this title”, “section 671(5) of this title” for “section 131(5) of this title”, and “section 659 of this title” for “section 148 of this title”.

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.”

§ 661. 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 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.

(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 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.)

CODIFICATION

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

AMENDMENTS

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

¹ So in original. Probably should be “51609”.