to include measures of intrusion and incident detection and response times.

(d) Transparency and accountability

The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, displaying metrics for department components, small agencies, and micro-agencies.

(e) Omitted

(f) Exception

The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(Pub. L. 114–113, div. N, title II, § 224, Dec. 18, 2015, 129 Stat. 2967.)

Editorial Notes

CODIFICATION

Section is comprised of section 224 of title II of div. N of Pub. L. 114–113. Subsec. (e) of section 224 of title II of div. N of Pub. L. 114–113 amended section 3553 of Title 44, Public Printing and Documents.

§ 1523. Federal cybersecurity requirements

(a) Implementation of Federal cybersecurity standards

Consistent with section 3553 of title 44, the Secretary, in consultation with the Director, shall exercise the authority to issue binding operational directives to assist the Director in ensuring timely agency adoption of and compliance with policies and standards promulgated under section 11331 of title 40 for securing agency information systems.

(b) Cybersecurity requirements at agencies

(1) In general

Consistent with policies, standards, guidelines, and directives on information security under subchapter II of chapter 35 of title 44 and the standards and guidelines promulgated under section 11331 of title 40 and except as provided in paragraph (2), not later than 1 year after December 18, 2015, the head of each agency shall—

(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44;

(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals' need to access the data;

(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

(E) implement identity management consistent with section 7464 of title 15, including multi-factor authentication, for—

(i) remote access to an agency information system; and

(ii) each user account with elevated privileges on an agency information system.

(2) Exception

The requirements under paragraph (1) shall not apply to an agency information system for which—

(A) the head of the agency has personally certified to the Director with particularity that—

(i) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the cybersecurity requirement;

(ii) the cybersecurity requirement is not necessary to secure the agency information system or agency information stored on or transiting it; and

(iii) the agency has taken all necessary steps to secure the agency information system and agency information stored on or transiting it; and

(B) the head of the agency or the designee of the head of the agency has submitted the certification described in subparagraph (A) to the appropriate congressional committees and the agency's authorizing committees.

(3) Construction

Nothing in this section shall be construed to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of chapter 35 of title 44. Nothing in this section shall be construed to affect the National Institute of Standards and Technology standards process or the requirement under section 3553(a)(4) of such title or to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.

(c) Exception

The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(Pub. L. 114–113, div. N, title II, § 225, Dec. 18, 2015, 129 Stat. 2967.)

§ 1524. Assessment; reports

(a) Definitions

In this section:

(1) Agency information

The term ''agency information'' has the meaning given the term in section 2213 of the Homeland Security Act of 2002 [6 U.S.C. 663].

(2) Cyber threat indicator; defensive measure

The terms ''cyber threat indicator'' and ''defensive measure'' have the meanings given those terms in section 1501 of this title.

(3) Intrusion assessments

The term ''intrusion assessments'' means actions taken under the intrusion assessment plan to identify and remove intruders in agency information systems.

(4) Intrusion assessment plan

The term ''intrusion assessment plan'' means the plan required under section 2210(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 660(b)(1)].

(5) Intrusion detection and prevention capabilities

The term ''intrusion detection and prevention capabilities'' means the capabilities required under section 2213(b) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)].

(b) Third-party assessment

Not later than 3 years after December 18, 2015, the Comptroller General of the United States shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan.

(c) Reports to Congress

(1) Intrusion detection and prevention capabilities

(A) Secretary of Homeland Security report

Not later than 6 months after December 18, 2015, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities, including—

(i) a description of privacy controls;

(ii) a description of the technologies and capabilities utilized to detect cybersecurity risks in network traffic, including the extent to which those technologies and capabilities include existing commercial and noncommercial technologies;

(iii) a description of the technologies and capabilities utilized to prevent network traffic associated with cybersecurity risks from transiting or traveling to or from agency information systems, including the extent to which those technologies and capabilities include existing commercial and noncommercial technologies;

(iv) a list of the types of indicators or other identifiers or techniques used to detect cybersecurity risks in network traffic transiting or traveling to or from agency information systems on each iteration of the intrusion detection and prevention capabilities and the number of each such type of indicator, identifier, and technique;

(v) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from agency information systems and the number of times the intrusion detection and prevention capabilities blocked network traffic associated with cybersecurity risk; and

(vi) a description of the pilot established under section 2213(c)(5) of the Homeland Security Act of 2002 [6 U.S.C. 663(c)(5)], including the number of new technologies tested and the number of participating agencies.

(B) OMB report

Not later than 18 months after December 18, 2015, and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, an analysis of agency application of the intrusion detection and prevention capabilities, including—

(i) a list of each agency and the degree to which each agency has applied the intrusion detection and prevention capabilities to an agency information system; and

(ii) a list by agency of—

(I) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such cybersecurity risks; and

(II) the number of instances in which the intrusion detection and prevention capabilities prevented network traffic associated with a cybersecurity risk from transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such agency information systems.

(C) Chief information officer

Not earlier than 18 months after December 18, 2015, and not later than 2 years after December 18, 2015, the Federal Chief Information Officer shall review and submit to the appropriate congressional committees a report assessing the intrusion detection and intrusion prevention capabilities, including—

(i) the effectiveness of the system in detecting, disrupting, and preventing cyberthreat actors, including advanced persistent threats, from accessing agency information and agency information systems;

(ii) whether the intrusion detection and prevention capabilities, continuous diagnostics and mitigation, and other systems deployed under subtitle D[1] of title II of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.) are effective in securing Federal information systems;

(iii) the costs and benefits of the intrusion detection and prevention capabilities, including as compared to commercial technologies and tools and including the value of classified cyber threat indicators; and

[1] See References in Text note below.

(iv) the capability of agencies to protect sensitive cyber threat indicators and defensive measures if they were shared through unclassified mechanisms for use in commercial technologies and tools.

(2) OMB report on development and implementation of intrusion assessment plan, advanced internal defenses, and Federal cybersecurity requirements

The Director shall—

(A) not later than 6 months after December 18, 2015, and 30 days after any update thereto, submit the intrusion assessment plan to the appropriate congressional committees;

(B) not later than 1 year after December 18, 2015, and annually thereafter, submit to Congress, as part of the report required under section 3553(c) of title 44—

(i) a description of the implementation of the intrusion assessment plan;

(ii) the findings of the intrusion assessments conducted pursuant to the intrusion assessment plan;

(iii) a description of the advanced network security tools included in the efforts to continuously diagnose and mitigate cybersecurity risks pursuant to section 1522(a)(1) of this title; and

(iv) a list by agency of compliance with the requirements of section 1523(b) of this title; and

(C) not later than 1 year after December 18, 2015, submit to the appropriate congressional committees—

(i) a copy of the plan developed pursuant to section 1522(a)(2) of this title; and

(ii) the improved metrics developed pursuant to section 1522(c) of this title.

(d) Form

Each report required under this section shall be submitted in unclassified form, but may include a classified annex.

(Pub. L. 114–113, div. N, title II, §226, Dec. 18, 2015, 129 Stat. 2969; Pub. L. 115–278, §2(h)(1)(F), Nov. 16, 2018, 132 Stat. 4182.)

Editorial Notes

REFERENCES IN TEXT

Subtitle D of title II of the Homeland Security Act of 2002, referred to in subsec. (c)(1)(C)(ii), is subtitle D (§§231–237) of title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2159, which enacted part D (§161 et seq.) of subchapter II of chapter 1 of this title and amended sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement. Subtitle D was redesignated subtitle C of title II of the Homeland Security Act of 2002 by Pub. L. 115–278, §2(g)(2)(K), Nov. 16, 2018, 132 Stat. 4178, and is classified principally to part C (§161 et seq.) of subchapter II of chapter 1 of this title. For complete classification of subtitle C to the Code, see Tables.

AMENDMENTS

2018—Subsec. (a)(1). Pub. L. 115–278, §2(h)(1)(F)(i)(I), substituted ''section 2213'' for ''section 230'' and struck out before period at end '', as added by section 223(a)(6) of this division''.

Subsec. (a)(4). Pub. L. 115–278, §2(h)(1)(F)(i)(II), substituted ''section 2210(b)(1)'' for ''section 228(b)(1)'' and struck out before period at end '', as added by section 223(a)(4) of this division''.

Subsec. (a)(5). Pub. L. 115–278, §2(h)(1)(F)(i)(III), substituted ''section 2213(b)'' for ''section 230(b)'' and struck out before period at end '', as added by section 223(a)(6) of this division''.

Subsec. (c)(1)(A)(vi). Pub. L. 115–278, §2(h)(1)(F)(ii), substituted ''section 2213(c)(5)'' for ''section 230(c)(5)'' and struck out '', as added by section 223(a)(6) of this division'' after ''Homeland Security Act of 2002''.

§ 1525. Termination

(a) In general

The authority provided under section 663 of this title, and the reporting requirements under section 1524(c) of this title shall terminate on the date that is 7 years after December 18, 2015.

(b) Rule of construction

Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under section 663(d)(2)[1] of this title, if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

(Pub. L. 114–113, div. N, title II, §227, Dec. 18, 2015, 129 Stat. 2971; Pub. L. 115–278, §2(h)(1)(G), Nov. 16, 2018, 132 Stat. 4182.)

Editorial Notes

AMENDMENTS

2018—Subsec. (a). Pub. L. 115–278, §2(h)(1)(G)(i), substituted ''section 663 of this title'' for ''section 151 of this title, as added by section 223(a)(6) of this division,''.

Subsec. (b). Pub. L. 115–278, §2(h)(1)(G)(ii), substituted ''section 663(d)(2) of this title'' for ''section 151(d)(2) of this title, as added by section 223(a)(6) of this division,''.

SUBCHAPTER III—OTHER CYBER MATTERS

§ 1531. Apprehension and prosecution of international cyber criminals

(a) International cyber criminal defined

In this section, the term ''international cyber criminal'' means an individual—

(1) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or the citizens of the United States; and

(2) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a ''Red Notice'') has been circulated by Interpol.

(b) Consultations for noncooperation

The Secretary of State, or designee, shall consult with the appropriate government official of each country from which extradition is not likely due to the lack of an extradition treaty with the United States or other reasons, in which one or more international cyber criminals are physically present, to determine what actions the government of such country has taken—

(1) to apprehend and prosecute such criminals; and

(2) to prevent such criminals from carrying out cybercrimes or intellectual property

[1] So in original. Probably should be ''663(c)(2)''.