6 USCS § 1524

Current through Public Law 118-62, approved May 13, 2024.

United States Code Service > TITLE 6. DOMESTIC SECURITY (§§ 101 — 1534) > CHAPTER 6. CYBERSECURITY (§§ 1500 — 1534) > FEDERAL CYBERSECURITY ENHANCEMENT (§§ 1521 — 1526)

§ 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 USCS § 663].

(2) Cyber threat indicator; defensive measure. The terms "cyber threat indicator" and "defensive measure" have the meanings given those terms in section 2200 of the Homeland Security Act of 2002 [6 USCS § 650].

(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 USCS § 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 USCS § 663(b)].

(b) Third-party assessment. Not later than 3 years after the date of enactment of this Act [enacted Dec. 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 the date of enactment of this Act [enacted Dec. 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 USCS § 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 the date of enactment of this Act [enacted Dec. 18, 2015], and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code, 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 the date of enactment of this Act [enacted Dec. 18, 2015] and not later than 2 years after the date of enactment of this Act [enacted Dec. 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 cyber-threat 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 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

(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 the date of enactment of this Act [enacted Dec. 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 the date of enactment of this Act [enacted Dec. 18, 2015], and annually thereafter, submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code—

(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 224(a)(1) [6 USCS § 1522(a)(1)]; and

(iv) a list by agency of compliance with the requirements of section 225(b) [6 USCS § 1523]; and

(C) not later than 1 year after the date of enactment of this Act [enacted Dec. 18, 2015], submit to the appropriate congressional committees—

(i) a copy of the plan developed pursuant to section 224(a)(2) [6 USCS § 1522(a)(2)]; and

(ii) the improved metrics developed pursuant to section 224(c) [6 USCS § 1522(c)].

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

History

HISTORY:

Dec. 18, 2015, P. L. 114-113, Div N, Title II, Subtitle B, § 226, 129 Stat. 2969; Nov. 16, 2018, P.L. 115-278, § 2(h)(1)(F), 132 Stat. 4182; Dec. 23, 2022, P.L. 117-263, Div G, Title LXXI, Subtitle E, § 7143(d)(1)(B), 136 Stat. 3663.

End of Document