(Pub. L. 114–113, div. N, title II, § 222, Dec. 18, 2015, 129 Stat. 2963; Pub. L. 115–278, § 2(h)(1)(D), Nov. 16, 2018, 132 Stat. 4182.)

Editorial Notes

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original ''this subtitle'', meaning subtitle B (§§ 221–229) of title II of div. N of Pub. L. 114–113, which is classified principally to this subchapter. For complete classification of subtitle B to the Code, see Tables.

AMENDMENTS

2018—Par. (2). Pub. L. 115–278, § 2(h)(1)(D)(i), substituted ''section 660 of this title'' for ''section 149 of this title, as added by section 223(a)(4) of this division''.

Par. (4). Pub. L. 115–278, § 2(h)(1)(D)(ii), substituted ''section 659 of this title'' for ''section 148 of this title, as so redesignated by section 223(a)(3) of this division''.

§ 1522. Advanced internal defenses

(a) Advanced network security tools

(1) In general

The Secretary shall include, in the efforts of the Department to continuously diagnose and mitigate cybersecurity risks, advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, and to detect and mitigate intrusions and anomalous activity.

(2) Development of plan

The Director shall develop and the Secretary shall implement a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.

(b) Prioritizing advanced security tools

The Director and the Secretary, in consultation with appropriate agencies, shall—

(1) review and update Government-wide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks; and

(2) brief appropriate congressional committees on such prioritization and use.

(c) Improved metrics

The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under section 3554 of title 44 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—