

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

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 230 of the Homeland Security Act of 2002 [6 U.S.C. 151], as added by section 223(a)(6) of this division.

(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 228(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 149(b)(1)], as added by section 223(a)(4) of this division.

(5) Intrusion detection and prevention capabilities

The term “intrusion detection and prevention capabilities” means the capabilities re-