

subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes—

- (A) computers and computer networks;
- (B) ancillary equipment;
- (C) software, firmware, and related procedures;
- (D) services, including support services; and
- (E) related resources.

(Added Pub. L. 107-296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2260.)

APPLICABILITY OF SECTION

This section not to apply while subchapter III of this chapter is in effect, see section 3549 of this title.

PRIOR PROVISIONS

A prior section 3532, added Pub. L. 106-398, §1 [[div. A], title X, §1061], Oct. 30, 2000, 114 Stat. 1654, 1654A-266, related to definitions applicable to this subchapter prior to the general amendment of this subchapter by Pub. L. 107-296.

§ 3533. Authority and functions of the Director

(a) The Director shall oversee agency information security policies and practices, by—

- (1) promulgating information security standards under section 11331 of title 40;
- (2) overseeing the implementation of policies, principles, standards, and guidelines on information security;
- (3) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—
 - (A) information collected or maintained by or on behalf of an agency; or
 - (B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
- (4) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;
- (5) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303(b)(5) of title 40, to enforce accountability for compliance with such requirements;
- (6) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3534(b);
- (7) coordinating information security policies and procedures with related information resources management policies and procedures; and

(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including—

- (A) a summary of the findings of evaluations required by section 3535;
- (B) significant deficiencies in agency information security practices;
- (C) planned remedial action to address such deficiencies; and
- (D) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(9) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

(b) Except for the authorities described in paragraphs (4) and (7) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

(Added Pub. L. 107-296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2261.)

APPLICABILITY OF SECTION

This section not to apply while subchapter III of this chapter is in effect, see section 3549 of this title.

PRIOR PROVISIONS

A prior section 3533, added Pub. L. 106-398, §1 [[div. A], title X, §1061], Oct. 30, 2000, 114 Stat. 1654, 1654A-266, set forth authority and functions of the Director prior to the general amendment of this subchapter by Pub. L. 107-296.

§ 3534. Federal agency responsibilities

(a) The head of each agency shall—

- (1) be responsible for—
 - (A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—
 - (i) information collected or maintained by or on behalf of the agency; and
 - (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
 - (B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—
 - (i) information security standards promulgated by the Director under section 11331 of title 40; and
 - (ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and
 - (C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;
- (2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—
 - (A) assessing the risk and magnitude of the harm that could result from the unau-