§ 3552. Definitions

(a) In general.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

(b) Additional definitions.—As used in this subchapter:

(1) The term ‘‘binding operational directive’’ means a compulsory direction to an agency that—

(A) is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk;

(B) shall be in accordance with policies, principles, standards, and guidelines issued by the Director; and

(C) may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director.

(2) The term ‘‘incident’’ means an occurrence that—

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies of an agency.

(3) The term ‘‘information security’’ means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

(4) The term ‘‘information technology’’ has the meaning given that term in section 11101 of title 40.

(5) The term ‘‘intelligence community’’ has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(6)(A) The term ‘‘national security system’’ means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or on behalf of an agency;

(B) information collected or maintained by or on behalf of an agency;

(C) information systems used or operated by an agency or by a contractor of an agency; or

(D) information collected or maintained by or on behalf of an agency.

(7) The term ‘‘Secretary’’ means the Secretary of Homeland Security.


PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3532 and 3542 of this title prior to repeal by Pub. L. 113–283.

§ 3553. Authority and Functions of the Director and the Secretary

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

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

(2) 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;

(3) ensuring that the Secretary carries out the authorities and functions under subsection (b); and

(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 11305 of title 40, to enforce accountability for compliance with such requirements; and

(6) coordinating information security policies and procedures with related information.