

EFFECTIVE DATE

Section effective May 22, 1995, see section 4 of Pub. L. 104-13, set out as a note under section 3501 of this title.

SUBCHAPTER II—INFORMATION SECURITY

APPLICABILITY OF SUBCHAPTER

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

AMENDMENTS

2002—Pub. L. 107-296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2259, reenacted subchapter heading without change.

§ 3531. Purposes

The purposes of this subchapter are to—

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

(4) provide a mechanism for improved oversight of Federal agency information security programs;

(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and

(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

(Added Pub. L. 107-296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2259.)

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 3531, added Pub. L. 106-398, §1 [[div. A], title X, §1061], Oct. 30, 2000, 114 Stat. 1654, 1654A-266, set forth purposes of this subchapter prior to the general amendment of this subchapter by Pub. L. 107-296.

EFFECTIVE DATE

Subchapter effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107-296, set out as a note under section 101 of Title 6, Domestic Security.

Pub. L. 106-398, §1 [[div. A], title X, §1065], Oct. 30, 2000, 114 Stat. 1654, 1654A-275, which provided that subtitle G (§§1061-1065) of title X of [div. A] of H.R. 5408, as enacted by section 1 of Pub. L. 106-398, enacting this

subchapter, amending sections 3501 to 3507, 3509, 3512, 3514 to 3518, and 3520 of this title, and section 2224 of Title 10, Armed Forces, and enacting provisions formerly set out as a note below, would take effect 30 days after Oct. 30, 2000, was repealed by Pub. L. 107-296, title X, §1005(b), Nov. 25, 2002, 116 Stat. 2272.

RESPONSIBILITIES OF CERTAIN AGENCIES

Pub. L. 106-398, §1 [[div. A], title X, §1062], Oct. 30, 2000, 114 Stat. 1654, 1654A-272, which set forth responsibilities of Department of Commerce, Department of Defense, Intelligence Community, Department of Justice, General Services Administration, and Office of Personnel Management relating to development, issuance, review, and updating of information security policies, principles, standards, and guidelines, including assessment of training and personnel needs, was repealed by Pub. L. 107-296, title X, §1005(b), Nov. 25, 2002, 116 Stat. 2272, and Pub. L. 107-347, title III, §305(b), Dec. 17, 2002, 116 Stat. 2960.

§ 3532. 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 “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;

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

(D) authentication, which means utilizing digital credentials to assure the identity of users and validate their access;

(2) 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 other organization on behalf of an agency, the function, operation, or use of which—

(A) involves intelligence activities;

(B) involves cryptologic activities related to national security;

(C) involves command and control of military forces;

(D) involves equipment that is an integral part of a weapon or weapons system; or

(E) is critical to the direct fulfillment of military or intelligence missions provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications);

(3) the term “information technology” has the meaning given that term in section 11101 of title 40; and

(4) the term “information system” means any equipment or interconnected system or