

compliance of that infrastructure with such policies, procedures, and practices, including automation of—

“(A) management, operational, and technical controls of every information system identified in the inventory required under section 3505(c) of title 44, United States Code; and

“(B) management, operational, and technical controls relied on for evaluations under [former] section 3545 of title 44, United States Code [see now 44 U.S.C. 3555].

“(b) DEFINITIONS.—In this section:

“(1) The term ‘information security incident’ means an occurrence that—

“(A) actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information such system processes, stores, or transmits; or

“(B) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies with respect to an information system.

“(2) The term ‘information infrastructure’ means the underlying framework, equipment, and software that an information system and related assets rely on to process, transmit, receive, or store information electronically.

“(3) The term ‘national security system’ has the meaning given that term in [former] section 3542(b)(2) of title 44, United States Code [see now 44 U.S.C. 3552(b)(6)].”

### [§ 2223a. Renumbered § 4571]

#### § 2224. Defense Information Assurance Program

(a) DEFENSE INFORMATION ASSURANCE PROGRAM.—The Secretary of Defense shall carry out a program, to be known as the “Defense Information Assurance Program”, to protect and defend Department of Defense information, information systems, and information networks that are critical to the Department and the armed forces during day-to-day operations and operations in times of crisis.

(b) OBJECTIVES OF THE PROGRAM.—The objectives of the program shall be to provide continuously for the availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Infrastructure.

(c) PROGRAM STRATEGY.—In carrying out the program, the Secretary shall develop a program strategy that encompasses those actions necessary to assure the readiness, reliability, continuity, and integrity of Defense information systems, networks, and infrastructure, including through compliance with subchapter II of chapter 35 of title 44, including through compliance with subchapter III of chapter 35 of title 44. The program strategy shall include the following:

(1) A vulnerability and threat assessment of elements of the defense and supporting non-defense information infrastructures that are essential to the operations of the Department and the armed forces.

(2) Development of essential information assurances technologies and programs.

(3) Organization of the Department, the armed forces, and supporting activities to defend against information warfare.

(4) Joint activities of the Department with other departments and agencies of the Government, State and local agencies, and elements of the national information infrastructure.

(5) The conduct of exercises, war games, simulations, experiments, and other activities designed to prepare the Department to respond to information warfare threats.

(6) Development of proposed legislation that the Secretary considers necessary for implementing the program or for otherwise responding to the information warfare threat.

(d) COORDINATION.—In carrying out the program, the Secretary shall coordinate, as appropriate, with the head of any relevant Federal agency and with representatives of those national critical information infrastructure systems that are essential to the operations of the Department and the armed forces on information assurance measures necessary to the protection of these systems.

[(e) Repealed. Pub. L. 108-136, div. A, title X, § 1031(a)(12), Nov. 24, 2003, 117 Stat. 1597.]

(f) INFORMATION ASSURANCE TEST BED.—The Secretary shall develop an information assurance test bed within the Department of Defense to provide—

(1) an integrated organization structure to plan and facilitate the conduct of simulations, war games, exercises, experiments, and other activities to prepare and inform the Department regarding information warfare threats; and

(2) organization and planning means for the conduct by the Department of the integrated or joint exercises and experiments with elements of the national information systems infrastructure and other non-Department of Defense organizations that are responsible for the oversight and management of critical information systems and infrastructures on which the Department, the armed forces, and supporting activities depend for the conduct of daily operations and operations during crisis.

(Added Pub. L. 106-65, div. A, title X, § 1043(a), Oct. 5, 1999, 113 Stat. 760; amended Pub. L. 106-398, § 1 [[div. A], title X, § 1063], Oct. 30, 2000, 114 Stat. 1654, 1654A-274; Pub. L. 107-296, title X, § 1001(c)(1)(B), Nov. 25, 2002, 116 Stat. 2267; Pub. L. 107-347, title III, § 301(c)(1)(B), Dec. 17, 2002, 116 Stat. 2955; Pub. L. 108-136, div. A, title X, § 1031(a)(12), Nov. 24, 2003, 117 Stat. 1597; Pub. L. 108-375, div. A, title X, § 1084(d)(17), Oct. 28, 2004, 118 Stat. 2062.)

#### Editorial Notes

##### AMENDMENTS

2004—Subsec. (c). Pub. L. 108-375 substituted “subchapter II” for “subtitle II” in introductory provisions.

2003—Subsec. (e). Pub. L. 108-136 struck out subsec. (e) which directed the Secretary of Defense to annually submit to Congress a report on the Defense Information Assurance Program.

2002—Subsec. (b). Pub. L. 107-296, § 1001(c)(1)(B)(i), and Pub. L. 107-347, § 301(c)(1)(B)(i), amended subsec. (b) identically, substituting “Objectives of the Program” for “Objectives and Minimum Requirements” in heading and striking out par. (1) designation before “The objectives”.

Subsec. (b)(2). Pub. L. 107-347, § 301(c)(1)(B)(ii), struck out par. (2) which read as follows: “The program shall at a minimum meet the requirements of sections 3534 and 3535 of title 44.”

Pub. L. 107-296, § 1001(c)(1)(B)(ii), which directed the striking out of “(2) the program shall at a minimum