

§ 2223. Information technology: additional responsibilities of Chief Information Officers

(a) ADDITIONAL RESPONSIBILITIES OF CHIEF INFORMATION OFFICER OF DEPARTMENT OF DEFENSE.—In addition to the responsibilities provided for in chapter 35 of title 44 and in section 11315 of title 40, the Chief Information Officer of the Department of Defense shall—

(1) review and provide recommendations to the Secretary of Defense on Department of Defense budget requests for information technology and national security systems;

(2) ensure the interoperability of information technology and national security systems throughout the Department of Defense;

(3) ensure that information technology and national security systems standards that will apply throughout the Department of Defense are prescribed;

(4) provide for the elimination of duplicate information technology and national security systems within and between the military departments and Defense Agencies; and

(5) maintain a consolidated inventory of Department of Defense mission critical and mission essential information systems, identify interfaces between those systems and other information systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems.

(b) ADDITIONAL RESPONSIBILITIES OF CHIEF INFORMATION OFFICER OF MILITARY DEPARTMENTS.—In addition to the responsibilities provided for in chapter 35 of title 44 and in section 11315 of title 40, the Chief Information Officer of a military department, with respect to the military department concerned, shall—

(1) review budget requests for all information technology and national security systems;

(2) ensure that information technology and national security systems are in compliance with standards of the Government and the Department of Defense;

(3) ensure that information technology and national security systems are interoperable with other relevant information technology and national security systems of the Government and the Department of Defense; and

(4) coordinate with the Joint Staff with respect to information technology and national security systems.

(c) DEFINITIONS.—In this section:

(1) The term “Chief Information Officer” means the senior official designated by the Secretary of Defense or a Secretary of a military department pursuant to section 3506 of title 44.

(2) The term “information technology” has the meaning given that term by section 11101 of title 40.

(3) The term “national security system” has the meaning given that term by section 3542(b)(2) of title 44.

(Added Pub. L. 105–261, div. A, title III, § 331(a)(1), Oct. 17, 1998, 112 Stat. 1967; amended Pub. L. 106–398, § 1 [[div. A], title VIII, § 811(a)], Oct. 30, 2000, 114 Stat. 1654, 1654A–210; Pub. L.

107–217, § 3(b)(1), Aug. 21, 2002, 116 Stat. 1295; Pub. L. 109–364, div. A, title IX, § 906(b), Oct. 17, 2006, 120 Stat. 2354.)

AMENDMENTS

2006—Subsec. (c)(3). Pub. L. 109–364 substituted “section 3542(b)(2) of title 44” for “section 11103 of title 40”.

2002—Subsecs. (a), (b). Pub. L. 107–217, § 3(b)(1)(A), (B), substituted “section 11315 of title 40” for “section 5125 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1425)” in introductory provisions.

Subsec. (c)(2). Pub. L. 107–217, § 3(b)(1)(C), substituted “section 11101 of title 40” for “section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401)”.

Subsec. (c)(3). Pub. L. 107–217, § 3(b)(1)(D), substituted “section 11103 of title 40” for “section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452)”.

2000—Subsec. (a)(5). Pub. L. 106–398 added par. (5).

EFFECTIVE DATE

Pub. L. 105–261, div. A, title III, § 331(b), Oct. 17, 1998, 112 Stat. 1968, provided that: “Section 2223 of title 10, United States Code, as added by subsection (a), shall take effect on October 1, 1998.”

CONTINUOUS MONITORING OF DEPARTMENT OF DEFENSE INFORMATION SYSTEMS FOR CYBERSECURITY

Pub. L. 111–383, div. A, title IX, § 931, Jan. 7, 2011, 124 Stat. 4334, provided that:

“(a) IN GENERAL.—The Secretary of Defense shall direct the Chief Information Officer of the Department of Defense to work, in coordination with the Chief Information Officers of the military departments and the Defense Agencies and with senior cybersecurity and information assurance officials within the Department of Defense and otherwise within the Federal Government, to achieve, to the extent practicable, the following:

“(1) The continuous prioritization of the policies, principles, standards, and guidelines developed 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) based upon the evolving threat of information security incidents with respect to national security systems, the vulnerability of such systems to such incidents, and the consequences of information security incidents involving such systems.

“(2) The automation of continuous monitoring of the effectiveness of the information security policies, procedures, and practices within the information infrastructure of the Department of Defense, and the 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 section 3545 of title 44, United States Code.

“(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 section 3542(b)(2) of title 44, United States Code.”

§ 2223a. Information technology acquisition planning and oversight requirements

(a) ESTABLISHMENT OF PROGRAM.—The Secretary of Defense shall establish a program to improve the planning and oversight processes for the acquisition of major automated information systems by the Department of Defense.

(b) PROGRAM COMPONENTS.—The program established under subsection (a) shall include—

(1) a documented process for information technology acquisition planning, requirements development and management, project management and oversight, earned value management, and risk management;

(2) the development of appropriate metrics that can be implemented and monitored on a real-time basis for performance measurement of—

(A) processes and development status of investments in major automated information system programs;

(B) continuous process improvement of such programs; and

(C) achievement of program and investment outcomes;

(3) a process to ensure that key program personnel have an appropriate level of experience, training, and education in the planning, acquisition, execution, management, and oversight of information technology systems;

(4) a process to ensure sufficient resources and infrastructure capacity for test and evaluation of information technology systems;

(5) a process to ensure that military departments and Defense Agencies adhere to established processes and requirements relating to the planning, acquisition, execution, management, and oversight of information technology programs and developments; and

(6) a process under which an appropriate Department of Defense official may intervene or terminate the funding of an information technology investment if the investment is at risk of not achieving major project milestones.

(Added Pub. L. 111-383, div. A, title VIII, § 805(a)(1), Jan. 7, 2011, 124 Stat. 4259.)

§ 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.)