sion authority for an information system described in subsection (c) may not provide Milestone A approval for the system unless, as part of the decision process for such approval, that authority determines that the system will achieve initial operational capability within a specified period of time not exceeding five years.

''(b) INITIAL OPERATIONAL CAPABILITY LIMITATION.—If an information system described in subsection (c), having received Milestone A approval, has not achieved initial operational capability within five years after the date of such approval, the system shall be deemed to have undergone a critical change in program requiring the evaluation and report required by section 2445c(d) of title 10, United States Code (as added by section 816 of this Act).

''(c) COVERED SYSTEMS.—An information system described in this subsection is any Department of Defense information technology business system that is not a national security system, as defined in 3542(b)(2) of title 44, United States Code.

''(d) DEFINITIONS.—In this section:

''(1) MILESTONE DECISION AUTHORITY.—The term 'milestone decision authority' has the meaning given that term in Department of Defense Instruction 5000.2, dated May 12, 2003.

''(2) MILESTONE A.—The term 'Milestone A' has the meaning given that term in Department of Defense Instruction 5000.2, dated May 12, 2003.''

§ 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.''

OZONE WIDGET FRAMEWORK

Pub. L. 112–81, div. A, title IX, § 924, Dec. 31, 2011, 125 Stat. 1539, provided that:

''(a) MECHANISM FOR INTERNET PUBLICATION OF INFORMATION FOR DEVELOPMENT OF ANALYSIS TOOLS AND APPLICATIONS.—The Chief Information Officer of the Department of Defense, acting through the Director of the Defense Information Systems Agency, shall implement a mechanism to publish and maintain on the public Internet the application programming interface specifications, a developer's toolkit, source code, and such other information on, and resources for, the Ozone Widget Framework (OWF) as the Chief Information Officer considers necessary to permit individuals and companies to develop, integrate, and test analysis tools and applications for use by the Department of Defense and the elements of the intelligence community.

''(b) PROCESS FOR VOLUNTARY CONTRIBUTION OF IMPROVEMENTS BY PRIVATE SECTOR.—In addition to the requirement under subsection (a), the Chief Information Officer shall also establish a process by which private individuals and companies may voluntarily contribute the following:

''(1) Improvements to the source code and documentation for the Ozone Widget Framework.

''(2) Alternative or compatible implementations of the published application programming interface specifications for the Framework.

''(c) ENCOURAGEMENT OF USE AND DEVELOPMENT.—The Chief Information Officer shall, whenever practicable, encourage and foster the use, support, development, and enhancement of the Ozone Widget Framework by the computer industry and commercial information technology vendors, including the development of tools that are compatible with the Framework.''

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.)

DATA SERVERS AND CENTERS

Pub. L. 112–81, div. B, title XXVIII, § 2867, Dec. 31, 2011, 125 Stat. 1704, provided that:

''(a) LIMITATIONS ON OBLIGATION OF FUNDS.—

''(1) LIMITATIONS.—

''(A) BEFORE PERFORMANCE PLAN.—During the period beginning on the date of the enactment of this Act [Dec. 31, 2011] and ending on May 1, 2012, a department, agency, or component of the Department of Defense may not obligate funds for a data server farm or data center unless approved by the Chief Information Officer of the Department of Defense or the Chief Information Officer of a component of the Department to whom the Chief Information Officer of the Department has specifically delegated such approval authority.

''(B) UNDER PERFORMANCE PLAN.—After May 1, 2012, a department, agency, or component of the Department may not obligate funds for a data center, or any information systems technology used therein, unless that obligation is in accordance with the performance plan required by subsection (b) and is approved as described in subparagraph (A).

''(2) REQUIREMENTS FOR APPROVALS.—

''(A) BEFORE PERFORMANCE PLAN.—An approval of the obligation of funds may not be granted under paragraph (1)(A) unless the official granting the approval determines, in writing, that existing resources of the agency, component, or element concerned cannot affordably or practically be used or modified to meet the requirements to be met through the obligation of funds.

''(B) UNDER PERFORMANCE PLAN.—An approval of the obligation of funds may not be granted under paragraph (1)(B) unless the official granting the approval determines that—

''(i) existing resources of the Department do not meet the operation requirements to be met through the obligation of funds; and

''(ii) the proposed obligation is in accordance with the performance standards and measures established by the Chief Information Officer of the Department under subsection (b).