''(c) REQUIRED ELEMENTS.—The Initiative shall include, to the maximum extent practicable—

''(1) the utilization of commercial, off-the-shelf technologies and web-based solutions;

''(2) a standardized technical environment and an open and accessible architecture; and

''(3) the implementation of common business processes, shared services, and common data structures.

''(d) STANDARDS.—In carrying out the Initiative, the Director of the Business Transformation Agency shall ensure that the Initiative is consistent with—

''(1) the requirements of the Business Enterprise Architecture and Transition Plan developed pursuant to section 2222 of title 10, United States Code;

''(2) the Standard Financial Information Structure of the Department of Defense;

''(3) the Federal Financial Management Improvement Act of 1996 [section 101(f) [title VIII] of title I of div. A of Pub. L. 104–208, 31 U.S.C. 3512 note] (and the amendments made by that Act); and

''(4) other applicable requirements of law and regulation.

''(e) SCOPE.—The Initiative shall be designed to provide, at a minimum, capabilities in the major process areas for both general fund and working capital fund operations of the Defense Agencies as follows:

''(1) Budget formulation.

''(2) Budget to report, including general ledger and trial balance.

''(3) Procure to pay, including commitments, obligations, and accounts payable.

''(4) Order to fulfill, including billing and accounts receivable.

''(5) Cost accounting.

''(6) Acquire to retire (account management).

''(7) Time and attendance and employee entitlement.

''(8) Grants financial management.

''(f) CONSULTATION.—In carrying out subsections (d) and (e), the Director of the Business Transformation Agency shall consult with the Comptroller of the Department of Defense [now Under Secretary of Defense (Comptroller)] to ensure that any financial management systems developed for the Defense Agencies, and any changes to the budget, finance, and accounting operations of the Defense Agencies, are consistent with the financial standards and requirements of the Department of Defense.

''(g) PROGRAM CONTROL.—In carrying out the Initiative, the Director of the Business Transformation Agency shall establish—

''(1) a board (to be known as the 'Configuration Control Board') to manage scope and cost changes to the Initiative; and

''(2) a program management office (to be known as the 'Program Management Office') to control and enforce assumptions made in the acquisition plan, the cost estimate, and the system integration contract for the Initiative, as directed by the Configuration Control Board.

''(h) PLAN ON DEVELOPMENT AND IMPLEMENTATION OF INITIATIVE.—Not later than six months after the date of the enactment of this Act [Jan. 28, 2008], the Director of the Business Transformation Agency shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a plan for the development and implementation of the Initiative. The plan shall provide for the implementation of an initial capability under the Initiative as follows:

''(1) In at least one Defense Agency by not later than eight months after the date of the enactment of this Act.

''(2) In not less than five Defense Agencies by not later than 18 months after the date of the enactment of this Act.''

LIMITATION ON FINANCIAL MANAGEMENT IMPROVEMENT AND AUDIT INITIATIVES WITHIN THE DEPARTMENT OF DEFENSE

Pub. L. 109–364, div. A, title III, § 321, Oct. 17, 2006, 120 Stat. 2144, as amended by Pub. L. 111–383, div. A, title X, § 1075(g)(1), Jan. 7, 2011, 124 Stat. 4376, provided that:

''(a) LIMITATION.—The Secretary of Defense may not obligate or expend any funds for the purpose of any financial management improvement activity relating to the preparation, processing, or auditing of financial statements until the Secretary submits to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a written determination that each activity proposed to be funded is—

''(1) consistent with the financial management improvement plan of the Department of Defense required by section 376(a)(1) of the National Defense Authorization Act for Fiscal Year 2006 (Public Law 109–163; 119 Stat. 3213); and

''(2) likely to improve internal controls or otherwise result in sustained improvements in the ability of the Department to produce timely, reliable, and complete financial management information.

''(b) EXCEPTION.—The limitation in subsection (a) shall not apply to an activity directed exclusively at assessing the adequacy of internal controls and remediating any inadequacy identified pursuant to such assessment.''

TIME-CERTAIN DEVELOPMENT FOR DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY BUSINESS SYSTEMS

Pub. L. 109–364, div. A, title VIII, § 811, Oct. 17, 2006, 120 Stat. 2316, which provided limitations for Milestone A approval and initial operational capability regarding certain Department of Defense information technology business systems, was repealed by Pub. L. 114–92, div. A, title VIII, § 883(c), Nov. 25, 2015, 129 Stat. 947.

§ 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 3552(b)(6) 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; Pub. L. 113–283, §2(e)(5)(B), Dec. 18, 2014, 128 Stat. 3087; Pub. L. 114–92, div. A, title X, §1081(a)(7), Nov. 25, 2015, 129 Stat. 1001.)

AMENDMENTS

2015—Subsec. (c)(3). Pub. L. 114–92 substituted ''section 3552(b)(6)'' for ''section 3552(b)(5)''.

2014—Subsec. (c)(3). Pub. L. 113–283 substituted ''section 3552(b)(5)'' for ''section 3542(b)(2)''.

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.''

PILOT PROGRAM ON EVALUATION OF COMMERCIAL INFORMATION TECHNOLOGY

Pub. L. 114–328, div. A, title II, §232, Dec. 23, 2016, 130 Stat. 2061, provided that:

''(a) PILOT PROGRAM.—The Director of the Defense Information Systems Agency may carry out a pilot program to evaluate commercially available information technology tools to better understand the potential impact of such tools on networks and computing environments of the Department of Defense.

''(b) ACTIVITIES.—Activities under the pilot program may include the following:

''(1) Prototyping, experimentation, operational demonstration, military user assessments, and other means of obtaining quantitative and qualitative feedback on the commercial information technology products.

''(2) Engagement with the commercial information technology industry to—

''(A) forecast military requirements and technology needs; and

''(B) support the development of market strategies and program requirements before finalizing acquisition decisions and strategies.

''(3) Assessment of novel or innovative commercial technology for use by the Department of Defense.

''(4) Assessment of novel or innovative contracting mechanisms to speed delivery of capabilities to the Armed Forces.

''(5) Solicitation of operational user input to shape future information technology requirements of the Department of Defense.

''(c) LIMITATION ON AVAILABILITY OF FUNDS.—Of the amounts authorized to be appropriated for research, development, test, and evaluation, Defense-wide, for each of fiscal years 2017 through 2022, not more than $15,000,000 may be expended on the pilot program in any such fiscal year.''

ADDITIONAL REQUIREMENTS RELATING TO THE SOFTWARE LICENSES OF THE DEPARTMENT OF DEFENSE

Pub. L. 113–66, div. A, title IX, §935, Dec. 26, 2013, 127 Stat. 833, provided that:

''(a) UPDATED PLAN.—

''(1) UPDATE.—The Chief Information Officer of the Department of the Defense shall, in consultation with the chief information officers of the military departments and the Defense Agencies, update the plan for the inventory of selected software licenses of the Department of Defense required under section 937 of the National Defense Authorization Act for 2013 [probably means the National Defense Authorization Act for Fiscal Year 2013] (Public Law 112–239; 10 U.S.C. 2223 note) to include a plan for the inventory of all software licenses of the Department of Defense for which a military department spends more than $5,000,000 annually on any individual title, including a comparison of licenses purchased with licenses in use.

''(2) ELEMENTS.—The update required under paragraph (1) shall—

''(A) include plans for implementing an automated solution capable of reporting the software license compliance position of the Department and providing a verified audit trail, or an audit trail otherwise produced and verified by an independent third party;

''(B) include details on the process and business systems necessary to regularly perform reviews, a procedure for validating and reporting deregistering and registering new software, and a mechanism and plan to relay that information to the appropriate chief information officer; and

''(C) a proposed timeline for implementation of the updated plan in accordance with paragraph (3).

''(3) SUBMISSION.—Not later than September 30, 2015, the Chief Information Officer of the Department of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] the updated plan required under paragraph (1).

''(b) PERFORMANCE PLAN.—If the Chief Information Officer of the Department of Defense determines through the implementation of the process and business systems in the updated plan required by subsection (a) that the number of software licenses of the Department for an individual title for which a military department spends greater than $5,000,000 annually exceeds the needs of the Department for such software licenses, or the inventory discloses that there is a discrepancy between the number of software licenses purchased and those in actual use, the Chief Information Officer of the Department of Defense shall implement a plan to bring the number of such software licenses into

balance with the needs of the Department and the terms of any relevant contract.''

COLLECTION AND ANALYSIS OF NETWORK FLOW DATA

Pub. L. 112–239, div. A, title IX, § 935, Jan. 2, 2013, 126 Stat. 1886, provided that:

''(a) DEVELOPMENT OF TECHNOLOGIES.—The Chief Information Officer of the Department of Defense may, in coordination with the Under Secretary of Defense for Policy and the Under Secretary of Defense for Intelligence and acting through the Director of the Defense Information Systems Agency, use the available funding and research activities and capabilities of the Community Data Center of the Defense Information Systems Agency to develop and demonstrate collection, processing, and storage technologies for network flow data that—

''(1) are potentially scalable to the volume used by Tier 1 Internet Service Providers to collect and analyze the flow data across their networks;

''(2) will substantially reduce the cost and complexity of capturing and analyzing high volumes of flow data; and

''(3) support the capability—

''(A) to detect and identify cyber security threats, networks of compromised computers, and command and control sites used for managing illicit cyber operations and receiving information from compromised computers;

''(B) to track illicit cyber operations for attribution of the source; and

''(C) to provide early warning and attack assessment of offensive cyber operations.

''(b) COORDINATION.—Any research and development required in the development of the technologies described in subsection (a) shall be conducted in cooperation with the heads of other appropriate departments and agencies of the Federal Government and, whenever feasible, Tier 1 Internet Service Providers and other managed security service providers.''

COMPETITION FOR LARGE-SCALE SOFTWARE DATABASE AND DATA ANALYSIS TOOLS

Pub. L. 112–239, div. A, title IX, § 936, Jan. 2, 2013, 126 Stat. 1886, provided that:

''(a) ANALYSIS.—

''(1) REQUIREMENT.—The Secretary of Defense, acting through the Chief Information Officer of the Department of Defense, shall conduct an analysis of large-scale software database tools and large-scale software data analysis tools that could be used to meet current and future Department of Defense needs for large-scale data analytics.

''(2) ELEMENTS.—The analysis required under paragraph (1) shall include—

''(A) an analysis of the technical requirements and needs for large-scale software database and data analysis tools, including prioritization of key technical features needed by the Department of Defense; and

''(B) an assessment of the available sources from Government and commercial sources to meet such needs, including an assessment by the Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy to ensure sufficiency and diversity of potential commercial sources.

''(3) SUBMISSION.—Not later than 180 days after the date of the enactment of this Act [Jan. 2, 2013], the Chief Information Officer shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] the results of the analysis required under paragraph (1).

''(b) COMPETITION REQUIRED.—

''(1) IN GENERAL.—If, following the analysis required under subsection (a), the Chief Information Officer of the Department of Defense identifies needs for software systems or large-scale software database or data analysis tools, the Department shall acquire such systems or such tools based on market research and using competitive procedures in accordance with applicable law and the Defense Federal Acquisition Regulation Supplement.

''(2) NOTIFICATION.—If the Chief Information Officer elects to acquire large-scale software database or data analysis tools using procedures other than competitive procedures, the Chief Information Officer and the Under Secretary of Defense for Acquisition, Technology, and Logistics shall submit a written notification to the congressional defense committees on a quarterly basis until September 30, 2018, that describes the acquisition involved, the date the decision was made, and the rationale for not using competitive procedures.''

SOFTWARE LICENSES OF THE DEPARTMENT OF DEFENSE

Pub. L. 112–239, div. A, title IX, § 937, Jan. 2, 2013, 126 Stat. 1887, provided that:

''(a) PLAN FOR INVENTORY OF LICENSES.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Jan. 2, 2013], the Chief Information Officer of the Department of the [sic] Defense shall, in consultation with the chief information officers of the military departments and the Defense Agencies, issue a plan for the inventory of selected software licenses of the Department of Defense, including a comparison of licenses purchased with licenses installed.

''(2) SELECTED SOFTWARE LICENSES.—The Chief Information Officer shall determine the software licenses to be treated as selected software licenses of the Department for purposes of this section. The licenses shall be determined so as to maximize the return on investment in the inventory conducted pursuant to the plan required by paragraph (1).

''(3) PLAN ELEMENTS.—The plan under paragraph (1) shall include the following:

''(A) An identification and explanation of the software licenses determined by the Chief Information Officer under paragraph (2) to be selected software licenses for purposes of this section, and a summary outline of the software licenses determined not to be selected software licenses for such purposes.

''(B) Means to assess the needs of the Department and the components of the Department for selected software licenses during the two fiscal years following the date of the issuance of the plan.

''(C) Means by which the Department can achieve the greatest possible economies of scale and cost savings in the procurement, use, and optimization of selected software licenses.

''(b) PERFORMANCE PLAN.—If the Chief Information Officer determines through the inventory conducted pursuant to the plan required by subsection (a) that the number of selected software licenses of the Department and the components of the Department exceeds the needs of the Department for such software licenses, the Secretary of Defense shall implement a plan to bring the number of such software licenses into balance with the needs of the Department.''

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 [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. 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.)

GUIDANCE ON ACQUISITION OF BUSINESS SYSTEMS

Pub. L. 114–92, div. A, title VIII, §883(e), Nov. 25, 2015, 129 Stat. 947, provided that: ''The Secretary of Defense shall issue guidance for major automated information systems acquisition programs to promote the use of best acquisition, contracting, requirement development, systems engineering, program management, and sustainment practices, including—

''(1) ensuring that an acquisition program baseline has been established within two years after program initiation;

''(2) ensuring that program requirements have not changed in a manner that increases acquisition costs or delays the schedule, without sufficient cause and only after maximum efforts to reengineer business processes prior to changing requirements;

''(3) policies to evaluate commercial off-the-shelf business systems for security, resilience, reliability, interoperability, and integration with existing interrelated systems where such system integration and interoperability are essential to Department of Defense operations;

''(4) policies to work with commercial off-the-shelf business system developers and owners in adapting systems for Department of Defense use;

''(5) policies to perform Department of Defense legacy system audits to determine which systems are related to or rely upon the system to be replaced or integrated with commercial off-the-shelf business systems;