''(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and initial operational capability regarding certain Department of Defense information technology business systems, was repealed by Pub.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.)

Editorial Notes

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).

Statutory Notes and Related Subsidiaries

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.''

MODERNIZATION OF THE DEPARTMENT OF DEFENSE'S AUTHORIZATION TO OPERATE PROCESSES

Pub. L. 118–159, div. A, title XV, § 1522, Dec. 23, 2024, 138 Stat. 2140, provided that:

''(a) ACTIVE DIRECTORY OF AUTHORIZING OFFICIALS.—

''(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act [Dec. 23, 2024], the Secretary of Defense, acting through the Chief Information Officer of the Department of Defense and in coordination with the Chief Information Officers of the military departments, shall establish and regularly update a digital directory of all authorizing officials in the military departments.

''(2) CONTENTS.—The directory established under paragraph (1) shall include—

''(A) the most current contact information for such authorizing official; and

''(B) a list of each training required to perform the duties and responsibilities of an authorizing official completed by such authorizing official.

''(b) PRESUMPTION OF RECIPROCAL SOFTWARE ACCREDITING STANDARDS.—

''(1) POLICY REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, acting through the Chief Information Officer of the Department of Defense, shall implement a policy that requires authorizing officials to adopt the security analysis and artifacts, as appropriate, of a cloud-hosted platform, service, or application that has already been authorized by another authorizing official in the Department of Defense in order to more rapidly adopt and use such cloud-hosted platforms, services, and applications, at the corresponding classification level and in accordance with the existing authorization conditions, without additional authorizations or reviews.

''(2) ELEMENTS.—The Secretary shall ensure that the policy implemented under paragraph (1)—

''(A) ensures the development of standardized and transparent documentation of the security, accreditation, performance, and operational capabilities of cloud-hosted platforms, services, and applications to enable decision making by mission owners of such cloud-hosted platforms, services, and applications;

''(B) provides for an intuitive and digital workflow to document acknowledgments among mission owners and system owners of use of the operational capabilities of cloud-hosted platforms, services, and applications;

''(C) directs a review by mission owners of existing authorization information, at the appropriate classification level, regarding the status of the operational capabilities of cloud-hosted platforms, services, and applications, including through management dashboards or other management analytic capabilities; and

''(D) defines a process, including required timelines, to allow authorizing officials that disagree with the security analysis of a cloud-hosted platform, service, or application that such official would be required to adopt under such policy to present such disagreement to the Chief Information Officer of the Department of Defense, or such other individual or entity designated by the Chief Information Officer, for adjudication.

''(3) APPLICABILITY.—The policy implemented pursuant to subsection (a) shall apply to—

''(A) all authorizing officials in the Department of Defense, including in each military department, component, and agency of the Department; and

''(B) all operational capabilities of cloud-hosted platforms, services, and applications, including capabilities on public cloud infrastructure, as authorized through the Federal Risk and Authorization Management Program established under section 3608 of title 44, United States Code, and the Defense Information Systems Agency, and capabilities on private cloud landing zones managed by the Department of Defense that are authorized by Department accrediting officials.

''(c) REPORT.—Not later than 120 days after the date of the enactment of this Act, the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the status of the implementation of subsections (a) and (b).

''(d) DEFINITIONS.—In this section—

''(1) the term 'Authorization to Operate' has the meaning given such term in the Office of Management and Budget Circular A-130;

''(2) the term 'authorizing official' means an officer who is authorized to assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the United States;

''(3) the term 'military departments' has the meaning given such term in section 101(a) of title 10, United States Code;

''(4) the term 'mission owner' means the user of a cloud-based platform, service, or application; and

''(5) the term 'system owner' means the element of the Department of Defense responsible for acquiring a cloud-based platform, service, or application, but which is not a mission owner of such cloud-based platform, service, or application.''

REQUIRED POLICIES TO ESTABLISH DATALINK STRATEGY OF DEPARTMENT OF DEFENSE

Pub. L. 118–31, div. A, title XV, § 1527, Dec. 22, 2023, 137 Stat. 559, provided that:

''(a) POLICIES REQUIRED.—

''(1) IN GENERAL.—The Secretary of Defense shall develop and implement policies to establish a unified datalink strategy of the Department of Defense (in this section referred to as the 'strategy').

''(2) ELEMENTS.—The policies under paragraph (1) shall provide for, at a minimum, the following:

''(A) The designation of an organization to serve as the lead coordinator of datalink activities throughout the Department of Defense.

''(B) The prioritization and coordination across the military departments with respect to the strategy within the requirements generation process of the Department.

''(C) The use throughout the Department of a common standardized datalink network or transport protocol that ensures interoperability between independently developed datalinks, regardless of physical medium used, and ensures mesh routing. In developing such policy, the Secretary of Defense shall consider the use of a subset of Internet Protocol.

''(D) A programmatic decoupling of the physical method used to transmit data, the network or transport protocols used in the transmission and reception of data, and the applications used to process and use data.

''(E) Coordination of the strategy with respect to weapon systems executing the same mission types across the military departments, including through the use of a common set of datalink waveforms. In developing such policy, the Secretary shall evaluate the use of redundant datalinks for line-of-sight and beyond-line-of-sight information exchange for each weapon systems platform.

''(F) Coordination between the Department and the intelligence community (as such term is defined in section 3 of the National Security Act of

1947 (50 U.S.C. 3003)) to leverage any efficiencies and overlap with existing datalink waveforms of the intelligence community.

''(G) Methods to support the rapid integration of common datalinks across the military departments.

''(H) Support for modularity of specific datalink waveforms to enable rapid integration of future datalinks, including the use of software defined radios compliant with modular open system architecture and sensor open system architecture.

''(b) INFORMATION TO CONGRESS.—Not later than June 1, 2024, the Secretary of Defense shall—

''(1) provide to the appropriate congressional committees a briefing on the proposed policies under subsection (a)(1), including timelines for the implementation of such policies; and

''(2) submit to the appropriate congressional committees—

''(A) an estimated timeline for the implementations of datalinks;

''(B) a list of any additional resources and authorities necessary to implement the strategy; and

''(C) a determination of whether a common set of datalinks can and should be implemented across all major weapon systems (as such term is defined in section 3455 of title 10, United States Code) of the Department of Defense.

''(c) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term 'appropriate congressional committees' means the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] and the congressional intelligence committees, as such term is defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).''

DEMONSTRATION PROGRAM FOR COMPONENT CONTENT MANAGEMENT SYSTEMS

Pub. L. 117–263, div. A, title IX, §917, Dec. 23, 2022, 136 Stat. 2756, provided that:

''(a) IN GENERAL.—Not later than July 1, 2023, the Chief Information Officer of the Department of Defense, in coordination with the official designated under section 238(b) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. note prec. 4061), shall complete a pilot program to demonstrate the application of component content management systems to a distinct set of data of the Department.

''(b) SELECTION OF DATA SET.—In selecting a distinct set of data of the Department for purposes of the pilot program required by subsection (a), the Chief Information Officer shall consult with, at a minimum, the following:

''(1) The Office of the Secretary of Defense, with respect to directives, instructions, and other regulatory documents of the Department.

''(2) The Office of the Secretary of Defense and the Joint Staff, with respect to execution orders.

''(3) The Office of the Under Secretary of Defense for Research and Engineering and the military departments, with respect to technical manuals.

''(4) The Office of the Under Secretary of Defense for Acquisition and Sustainment, with respect to Contract Data Requirements List documents.

''(c) AUTHORITY TO ENTER INTO CONTRACTS.—Subject to the availability of appropriations, the Secretary of Defense may enter into contracts or other agreements with public or private entities to conduct studies and demonstration projects under the pilot program required by subsection (a).

''(c) [sic] BRIEFING REQUIRED.—Not later than 60 days after the date of the enactment of this Act [Dec. 23, 2022], the Chief Information Officer shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on plans to implement the pilot program required by subsection (a).

''(d) COMPONENT CONTENT MANAGEMENT SYSTEM DEFINED.—In this section, the term 'component content management system' means any content management system that enables the management of content at a component level instead of at the document level.''

IMPROVED MANAGEMENT OF INFORMATION TECHNOLOGY AND CYBERSPACE INVESTMENTS

Pub. L. 116–92, div. A, title VIII, §892, Dec. 20, 2019, 133 Stat. 1539, provided that:

''(a) IMPROVED MANAGEMENT.—

''(1) IN GENERAL.—The Chief Information Officer of the Department of Defense shall work with the Chief Data Officer of the Department of Defense to optimize the Department's process for accounting for, managing, and reporting its information technology and cyberspace investments. The optimization should include alternative methods of presenting budget justification materials to the public and congressional staff to more accurately communicate when, how, and with what frequency capability is delivered to end users, in accordance with best practices for managing and reporting on information technology investments.

''(2) BRIEFING.—Not later than February 3, 2020, the Chief Information Officer of the Department of Defense shall brief the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] on the process optimization undertaken pursuant to paragraph (1), including any recommendations for legislation.

''(b) DELIVERY OF INFORMATION TECHNOLOGY BUDGET.—The Secretary of Defense shall submit to the congressional defense committees the Department of Defense budget request for information technology not later than 15 days after the submittal to Congress of the budget of the President for a fiscal year pursuant to section 1105 of title 31, United States Code.''

CHIEF DATA OFFICER RESPONSIBILITY FOR DOD DATA SETS

Pub. L. 116–92, div. A, title IX, §903(b), Dec. 20, 2019, 133 Stat. 1555, as amended by Pub. L. 117–263, div. A, title II, §212(k), Dec. 23, 2022, 136 Stat. 2470, provided that:

''(1) IN GENERAL.—In addition to any other functions and responsibilities specified in section 3520(c) of title 44, United States, Code, the Chief Data Officer of the Department of Defense shall also be the official in the Department of Defense with principal responsibility for providing for the availability of common, usable, Defense-wide data sets.

''(2) ACCESS TO ALL DOD DATA.—In order to carry out the responsibility specified in paragraph (1), the Chief Data Officer shall have access to all Department of Defense data, including data in connection with warfighting missions and back-office data.

''(3) REPORT.—Not later than December 1, 2019, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report setting forth such recommendations for legislative or administrative action as the Secretary considers appropriate to carry out this subsection.''

PILOT PROGRAM FOR OPEN SOURCE SOFTWARE

Pub. L. 115–91, div. A, title VIII, §875, Dec. 12, 2017, 131 Stat. 1503, provided that:

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 12, 2017], the Secretary of Defense shall initiate for the Department of Defense the open source software pilot program established by the Office of Management and Budget Memorandum M-16-21 titled 'Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software' and dated August 8, 2016.

''(b) REPORT TO CONGRESS.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Defense shall provide a report to Congress

with details of the plan of the Department of Defense to implement the pilot program required by subsection (a). Such plan shall include identifying candidate software programs, selection criteria, intellectual property and licensing issues, and other matters determined by the Secretary.

''(c) COMPTROLLER GENERAL REPORT.—Not later than June 1, 2019, the Comptroller General of the United States shall provide a report to Congress on the implementation of the pilot program required by subsection (a) by the Secretary of Defense. The report shall address, at a minimum, the compliance of the Secretary with the requirements of the Office of Management and Budget Memorandum M-16-21, the views of various software and information technology stakeholders in the Department of Defense, and any other matters determined by the Comptroller General.''

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 [now Under Secretary of Defense for Intelligence and Security] 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. 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 nondefense 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