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.)

IMPLEMENTATION OF RECOMMENDATIONS OF THE FINAL REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON THE DESIGN AND ACQUISITION OF SOFTWARE FOR DEFENSE SYSTEMS

Pub. L. 115–232, div. A, title VIII, § 868, Aug. 13, 2018, 132 Stat. 1902, provided that:

''(a) IMPLEMENTATION REQUIRED.—Not later than 18 months after the date of the enactment of this Act [Aug. 13, 2018], the Secretary of Defense shall, except as provided under subsection (b), commence implementation of each recommendation submitted as part of the final report of the Defense Science Board Task Force on the Design and Acquisition of Software for Defense Systems.

''(b) EXCEPTIONS.—

''(1) DELAYED IMPLEMENTATION.—The Secretary of Defense may commence implementation of a recommendation described under subsection (a) later than the date required under such subsection if the Secretary provides the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] with a specific justification for the delay in implementation of such recommendation.

''(2) NONIMPLEMENTATION.—The Secretary of Defense may opt not to implement a recommendation described under subsection (a) if the Secretary provides to the congressional defense committees—

''(A) the reasons for the decision not to implement the recommendation; and

''(B) a summary of the alternative actions the Secretary plans to take to address the purposes underlying the recommendation.

''(c) IMPLEMENTATION PLANS.—For each recommendation that the Secretary is implementing, or that the Secretary plans to implement, the Secretary shall submit to the congressional defense committees—

''(1) a summary of actions that have been taken to implement the recommendation; and

''(2) a schedule, with specific milestones, for completing the implementation of the recommendation.''

ACTIVITIES AND REPORTING RELATING TO DEPARTMENT OF DEFENSE'S CLOUD INITIATIVE

Pub. L. 115–232, div. A, title X, § 1064, Aug. 13, 2018, 132 Stat. 1971, provided that:

''(a) ACTIVITIES REQUIRED.—Commencing not later than 90 days after the date of the enactment of this Act [Aug. 13, 2018], the Chief Information Officer of the Department of Defense, acting through the Cloud Executive Steering Group established by the Deputy Secretary of Defense in a directive memorandum dated September 13, 2017, in order to support its Joint Enterprise Defense Infrastructure initiative to procure commercial cloud services, shall conduct certain key enabling activities as follows:

''(1) Develop an approach to rapidly acquire advanced commercial network capabilities, including software-defined networking, on-demand bandwidth, and aggregated cloud access gateways, through commercial service providers in order—

''(A) to support the migration of applications and systems to commercial cloud platforms;

''(B) to increase visibility of end-to-end performance to enable and enforce service level agreements for cloud services;

''(C) to ensure efficient and common cloud access;

''(D) to facilitate shifting data and applications from one cloud platform to another;

''(E) to improve cybersecurity; and

''(F) to consolidate networks and achieve efficiencies and improved performance;

''(2) Conduct an analysis of existing workloads that would be migrated to the Joint Enterprise Defense Infrastructure, including—

''(A) identifying all of the cloud initiatives across the Department of Defense, and determining the objectives of such initiatives in connection with the intended scope of the Infrastructure;

''(B) identifying all the systems and applications that the Department would intend to migrate to the Infrastructure;

''(C) conducting rationalization of applications to identify applications and systems that may duplicate the processing of workloads in connection with the Infrastructure; and

''(D) as result of such actions, arriving at dispositions about migration or termination of systems and applications in connection with the Infrastructure.

''(b) REPORT REQUIRED.—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] a report on the Department of Defense's Cloud Initiative to manage networks, data centers, and clouds at the enterprise level. Such report shall include each of the following:

''(1) A description [of] the status of completion of the activities required under subsection (a).

''(2) Information relating to the current composition of the Cloud Executive Steering Group and the stakeholders relating to the Department of Defense's Cloud Initiative and associated mission, objectives, goals, and strategy.

''(3) A description of the characteristics and considerations for accelerating the cloud architecture and services required for a global, resilient, and secure information environment.

''(4) Information relating to acquisition strategies and timeline for efforts associated with the Department of Defense's Cloud Initiative, including the Joint Enterprise Defense Infrastructure.

''(5) A description of how the acquisition strategies referred to in paragraph (4) provides [sic] for a full and open competition, enable the Department of Defense to continuously leverage and acquire new cloud computing capabilities, maintain the ability of the Department to leverage other cloud computing vendor products and services, incorporate elements to maintain security, and provide for the best performance, cost, and schedule to meet the cloud architecture and services requirements of the Department for the duration of such contract.

''(6) A detailed description of existing workloads that will be migrated to enterprise-wide cloud infrastructure or platforms as a result of the Department of Defense's Cloud Initiative, including estimated migration costs and timelines, based on the analysis required under subsection (a)(2).

''(7) A description of the program management and program office of the Department of Defense's Cloud Initiative, including the number of personnel, overhead costs, and organizational structure.

''(8) A description of the effect of the Joint Enterprise Defense Infrastructure on and the relationship of such Infrastructure to existing cloud computing infrastructure, platform, and service contracts across the Department of Defense, specifically the effect and relationship to the private cloud infrastructure of the Department, MilCloud 2.0 run by the Defense Information Systems Agency based on the analysis required under subsection (a)(2).

''(9) Information relating to the most recent Department of Defense Cloud Computing Strategy and description of any initiatives to update such Strategy.

''(10) Information relating to Department of Defense guidance pertaining to cloud computing capability or platform acquisition and standards, and a description of any initiatives to update such guidance.

''(11) Any other matters the Secretary of Defense determines relevant.

''(c) LIMITATION ON USE OF FUNDS.—Of the amounts authorized to be appropriated or otherwise made available by this Act [see Tables for classification] for fiscal

year 2019 for the Department of Defense's Cloud Initiative, not more than 85 percent may be obligated or expended until the Secretary of Defense submits to the congressional defense committees the report required by subsection (b).

''(d) LIMITATION ON NEW SYSTEMS AND APPLICATIONS.—

''(1) IN GENERAL.—Except as provided in paragraph (2), the Deputy Secretary shall require that no new system or application will be approved for development or modernization without an assessment that such system or application is already, or can and would be, cloud-hosted.

''(2) WAIVER.—The Deputy Secretary may issue a national waiver to the requirement under paragraph (1) if the Deputy Secretary determines, pursuant to the assessment described in such paragraph, that the requirement would adversely affect the national security of the United States. If the Deputy Secretary issues a waiver under this paragraph, the Deputy Secretary shall provide to the congressional defense committees a written notification of such waiver, justification for the waiver, and identification of the system or application to which the waiver applies by not later than 15 days after the date on which the waiver is issued.

''(e) TRANSPARENCY AND COMPETITION.—The Deputy Secretary shall ensure that the acquisition approach of the Department continues to follow the Federal Acquisition Regulation with respect to competition.''

PILOT PROGRAM TO USE AGILE OR ITERATIVE DEVELOPMENT METHODS TO TAILOR MAJOR SOFTWARE-INTENSIVE WARFIGHTING SYSTEMS AND DEFENSE BUSINESS SYSTEMS

Pub. L. 115–232, div. A, title VIII, §869(a)–(d), Aug. 13, 2018, 132 Stat. 1902, 1903, provided that:

''(a) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act [Aug. 13, 2018], the Secretary of Defense shall include the following systems in the pilot program to use agile or iterative development methods pursuant to section 873 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 10 U.S.C. 2223a note):

''(1) Defense Retired and Annuitant Pay System 2 (DRAS2), Defense Logistics Agency.

''(2) Army Integrated Air and Missile Defense (AIAMD), Army.

''(3) Army Contract Writing System (ACWS), Army.

''(4) Defense Enterprise Accounting and Management System (DEAMS) Inc2, Air Force.

''(5) Item Master, Air Force.

''(b) ADDITIONS TO LIST.—Not later than 30 days after the date of the enactment of this Act, the Secretary of Defense shall identify three additional systems for participation in the pilot program pursuant to section 873 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 10 U.S.C. 2223a note) and notify the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] of the additions.

''(c) COMMUNITY OF PRACTICE ADVISING ON AGILE OR ITERATIVE DEVELOPMENT.—The Under Secretary of Defense for Acquisition and Sustainment shall establish a Community of Practice on agile or iterative methods so that programs that have been incorporating agile or iterative methods can share with programs participating in the pilot the lessons learned, best practices, and recommendations for improvements to acquisition and supporting processes. The Service Acquisition Executives of the military departments shall send representation from the following programs, which have reported using agile or iterative methods:

''(1) Air and Space Operations Center (AOC).

''(2) Command Control Battle Management and Communications (C2BMC).

''(3) The family of Distributed Common Ground Systems.

''(4) The family of Global Command and Control Systems.

''(5) Navy Personnel and Pay (NP2).

''(6) Other programs and activities as appropriate.

''(d) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall report to the congressional defense committees on the status of the pilot program and each system participating in the pilot. The report shall include the following elements:

''(1) A description of how cost and schedule estimates in support of the program are being conducted and using what methods.

''(2) The contracting strategy and types of contracts that will be used in executing the program.

''(3) A description of how intellectual property ownership issues associated with software applications developed with agile or iterative methods will be addressed to ensure future sustainment, maintenance, and upgrades to software applications after the applications are fielded.

''(4) A description of the tools and software applications that are expected to be developed for the program and the costs and cost categories associated with each.

''(5) A description of challenges the program has faced in realigning the program to use agile or iterative methods.''

Pub. L. 115–91, div. A, title VIII, §873, Dec. 12, 2017, 131 Stat. 1498, as amended by Pub. L. 115–232, div. A, title VIII, §869(e), Aug. 13, 2018, 132 Stat. 1903, provided that:

''(a) PILOT PROGRAM.—

''(1) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act [Dec. 12, 2017], the Secretary of Defense, in consultation with the Secretaries of the military departments and the chiefs of the armed forces, shall establish a pilot program to tailor and simplify software development requirements and methods for major software-intensive warfighting systems and defense business systems.

''(2) IMPLEMENTATION PLAN FOR PILOT PROGRAM.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Defense, in consultation with the Secretaries of the military departments and the chiefs of the armed forces, shall develop a plan for implementing the pilot program required under this subsection, including guidance for implementing the program and for selecting systems for participation in the program.

''(3) SELECTION OF SYSTEMS FOR PILOT PROGRAM.—

''(A) The implementation plan shall require that systems be selected as follows:

''(i) For major software-intensive warfighting systems, one system per armed force and one defense-wide system, including at least one major defense acquisition program or major automated information system.

''(ii) For defense business systems, not fewer than two systems and not greater than eight systems.

''(B) In selecting systems or subsystems for participation, the Secretary shall prioritize systems as follows:

''(i) For major software-intensive warfighting systems, systems that—

''(I) have identified software development as a high risk;

''(II) have experienced cost growth and schedule delay; or

''(III) did not deliver any operational capability within the prior calendar year.

''(ii) For defense business systems, systems that—

''(I) have experienced cost growth and schedule delay;

''(II) did not deliver any operational capability within the prior calendar year; or

''(III) are underperforming other systems within a defense business system portfolio with similar user requirements.

''(b) REALIGNMENT PLANS.—

''(1) IN GENERAL.—Not later than 60 days after selecting a system for the pilot program under sub-

section (a)(3), the Secretary shall develop a plan for realigning the system by breaking down the system into smaller increments using agile or iterative development methods. The realignment plan shall include a revised cost estimate that is lower than the cost estimate for the system that was current as of the date of the enactment of this Act [Dec. 12, 2017].

''(2) REALIGNMENT EXECUTION.—Each increment for a realigned system shall—

''(A) be designed to deliver a meaningfully useful capability within the first 180 days following realignment;

''(B) be designed to deliver subsequent meaningfully useful capabilities in time periods of less than 180 days;

''(C) incorporate multidisciplinary teams focused on software production that prioritize user needs and control of total cost of ownership;

''(D) be staffed with highly qualified technically trained staff and personnel with management and business process expertise in leadership positions to support requirements modification, acquisition strategy, and program decisionmaking;

''(E) ensure that the acquisition strategy for the realigned system is broad enough to allow for proposals of a service, system, modified business practice, configuration of personnel, or combination thereof for implementing the strategy;

''(F) include periodic engagement with the user community, as well as representation by the user community in program management and software production activity;

''(G) ensure that the acquisition strategy for the realigned system favors outcomes-based requirements definition and capability as a service, including the establishment of technical evaluation criteria as outcomes to be used to negotiate service-level agreements with vendors; and

''(H) consider options for termination of the relationship with any vendor unable or unwilling to offer terms that meet the requirements of this section.

''(c) REMOVAL OF SYSTEMS.—The Secretary may remove a system selected for the pilot program under subsection (a)(3) only after the Secretary submits to the Committees on Armed Services of the Senate and House of Representatives a written determination that indicates that the selected system has been unsuccessful in reducing cost or schedule growth, or is not meeting the overall needs of the pilot program.

''(d) EDUCATION AND TRAINING IN AGILE OR ITERATIVE DEVELOPMENT METHODS.—

''(1) TRAINING REQUIREMENT.—The Secretary shall ensure that any personnel from the relevant organizations in each of the military departments and Defense Agencies participating in the pilot program, including organizations responsible for engineering, budgeting, contracting, test and evaluation, requirements validation, and certification and accreditation, receive targeted training in agile or iterative development methods, including the interim course required by section 891 of this Act [10 U.S.C. 1746 note].

''(2) SUPPORT.—In carrying out the pilot program under subsection (a), the Secretary shall ensure that personnel participating in the program provide feedback to inform the development of education and training curricula as required by section 891.

''(e) SUNSET.—The pilot program required under subsection (a) shall terminate on September 30, 2023. Any system selected under subsection (a)(3) for the pilot program shall continue after that date through the execution of its realignment plan.

''(f) AGILE OR ITERATIVE DEVELOPMENT DEFINED.—In this section, the term 'agile or iterative development', with respect to software—

''(1) means acquisition pursuant to a method for delivering multiple, rapid, incremental capabilities to the user for operational use, evaluation, and feedback not exclusively linked to any single, proprietary method or process; and

''(2) involves—

''(A) the incremental development and fielding of capabilities, commonly called 'spirals', 'spins', or 'sprints', which can be measured in a few weeks or months; and

''(B) continuous participation and collaboration by users, testers, and requirements authorities.''

GLOBAL THEATER SECURITY COOPERATION MANAGEMENT INFORMATION SYSTEM

Pub. L. 115–91, div. A, title XII, § 1272, Dec. 12, 2017, 131 Stat. 1695, provided that:

''(a) UPDATE OF GUIDANCE.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 12, 2017], the Secretary of Defense shall—

''(A) update relevant security cooperation guidance issued by the Secretary for use of the Global Theater Security Cooperation Management Information System (in this section referred to as 'G-TSCMIS'), including guidance relating to the matters described in paragraph (3); and

''(B) submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report that contains such guidance.

''(2) SUCCESSOR SYSTEM.—Not later than 180 days after the date of the adoption of any security cooperation information system that is a successor to G-TSCMIS, the Secretary of Defense shall—

''(A) update relevant security cooperation guidance issued by the Secretary for use of such system, including guidance relating to the matters described in paragraph (3); and

''(B) submit to the congressional defense committees a report that contains such guidance.

''(3) MATTERS DESCRIBED.—The matters described in this paragraph are the following:

''(A) Designation of an authoritative data repository for security cooperation information, with enforceable data standards and data controls.

''(B) Responsibilities for entry of data relating to programs and activities into the system.

''(C) Oversight and accountability measures to ensure the full scope of activities are entered into the system consistently and in a timely manner.

''(D) Such other matters as the Secretary considers appropriate.

''(b) REPORT.—

''(1) IN GENERAL.—Not later than 270 days after the adoption of any security cooperation information system that is the successor to G-TSCMIS, the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report setting forth a review of measures for evaluating the system in order to comply with guidance required by subsection (a).

''(2) ELEMENTS.—The review required by paragraph (1) shall include the following:

''(A) An evaluation of the impacts of inconsistent information on the system's functionality as a tool for planning, resource allocation, and adjustment.

''(B) An evaluation of the effectiveness of oversight and accountability measures.

''(C) An evaluation of feedback from the operational community to inform future requirements.

''(D) Such other matters as the Secretary considers appropriate.

''(3) FORM.—The report required under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.''

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 develop-

ment, 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;

''(6) policies to perform full backup of systems that will be changed or replaced by the installation of commercial off-the-shelf business systems prior to installation and deployment to ensure reconstitution of the system to a functioning state should it become necessary;

''(7) policies to engage the research and development activities and laboratories of the Department of Defense to improve acquisition outcomes; and

''(8) policies to refine and improve developmental and operational testing of business processes that are supported by the major automated information systems.''

DESIGNATION OF MILITARY DEPARTMENT ENTITY RESPONSIBLE FOR ACQUISITION OF CRITICAL CYBER CAPABILITIES

Pub. L. 114–92, div. A, title XVI, §1645, Nov. 25, 2015, 129 Stat. 1117, provided that:

''(a) DESIGNATION.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act [Nov. 25, 2015], the Secretary of Defense shall designate an entity within a military department to be responsible for the acquisition of each critical cyber capability described in paragraph (2).

''(2) CRITICAL CYBER CAPABILITIES DESCRIBED.—The critical cyber capabilities described in this paragraph are the cyber capabilities that the Secretary considers critical to the mission of the Department of Defense, including the following:

''(A) The Unified Platform described in the Department of Defense document titled 'The Department of Defense Cyber Strategy' dated April 15, 2015.

''(B) A persistent cyber training environment.

''(C) A cyber situational awareness and battle management system.

''(b) REPORT.—

''(1) IN GENERAL.—Not later than 90 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 containing the information described in paragraph (2).

''(2) CONTENTS.—The report under paragraph (1) shall include the following with respect to the critical cyber capabilities described in subsection (a)(2):

''(A) Identification of each critical cyber capability and the entity of a military department responsible for the acquisition of the capability.

''(B) Estimates of the funding requirements and acquisition timelines for each critical cyber capability.

''(C) An explanation of whether critical cyber capabilities could be acquired more quickly with changes to acquisition authorities.

''(D) Such recommendations as the Secretary may have for legislation or administrative action to improve the acquisition of, or to acquire more quickly, the critical cyber capabilities for which designations are made under subsection (a).''

MODULAR OPEN SYSTEMS APPROACHES IN ACQUISITION PROGRAMS

Pub. L. 113–291, div. A, title VIII, §801, Dec. 19, 2014, 128 Stat. 3425, provided that:

''(a) PLAN FOR MODULAR OPEN SYSTEMS APPROACH THROUGH DEVELOPMENT AND ADOPTION OF STANDARDS AND ARCHITECTURES.—Not later than January 1, 2016, the Under Secretary of Defense for Acquisition, Technology, and Logistics shall submit a report to the Committees on Armed Services of the Senate and the House of Representatives detailing a plan to develop standards and define architectures necessary to enable open systems approaches in the key mission areas of the Department of Defense with respect to which the Under Secretary determines that such standards and architectures would be feasible and cost effective.

''(b) CONSIDERATION OF MODULAR OPEN SYSTEMS APPROACHES.—

''(1) Review of acquisition guidance.—The Under Secretary of Defense for Acquisition, Technology, and Logistics shall review current acquisition guidance, and modify such guidance as necessary, to—

''(A) ensure that acquisition programs include open systems approaches in the product design and acquisition of information technology systems to the maximum extent practicable; and

''(B) for any information technology system not using an open systems approach, ensure that written justification is provided in the contract file for the system detailing why an open systems approach was not used.

''(2) ELEMENTS.—The review required in paragraph (1) shall—

''(A) consider whether the guidance includes appropriate exceptions for the acquisition of—

''(i) commercial items; and

''(ii) solutions addressing urgent operational needs;

''(B) determine the extent to which open systems approaches should be addressed in analysis of alternatives, acquisition strategies, system engineering plans, and life cycle sustainment plans; and

''(C) ensure that increments of acquisition programs consider the extent to which the increment will implement open systems approaches as a whole.

''(3) DEADLINE FOR REVIEW.—The review required in this subsection shall be completed no later than 180 days after the date of the enactment of this Act [Dec. 19, 2014].

''(c) TREATMENT OF ONGOING AND LEGACY PROGRAMS.—

''(1) REPORT REQUIREMENT.—Not later than one year after the date of the enactment of this Act, the Under Secretary of Defense for Acquisition, Technology, and Logistics shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report covering the matters specified in paragraph (2).

''(2) MATTERS COVERED.—Subject to paragraph (3), the report required in this subsection shall—

''(A) identify all information technology systems that are in development, production, or deployed status as of the date of the enactment of this Act, that are or were major defense acquisition programs or major automated information systems, and that are not using an open systems approach;

''(B) identify gaps in standards and architectures necessary to enable open systems approaches in the key mission areas of the Department of Defense, as determined pursuant to the plan submitted under subsection (a); and

''(C) outline a process for potential conversion to an open systems approach for each information technology system identified under subparagraph (A).

''(3) LIMITATIONS.—The report required in this subsection shall not include information technology systems—

''(A) having a planned increment before fiscal year 2021 that will result in conversion to an open systems approach; and

''(B) that will be in operation for fewer than 15 years after the date of the enactment of this Act.

''(d) DEFINITIONS.—In this section:

''(1) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101(6) of title 40, United States Code.

''(2) OPEN SYSTEMS APPROACH.—The term 'open systems approach' means, with respect to an information technology system, an integrated business and technical strategy that—

''(A) employs a modular design and uses widely supported and consensus-based standards for key interfaces;

''(B) is subjected to successful validation and verification tests to ensure key interfaces comply with widely supported and consensus-based standards; and

''(C) uses a system architecture that allows components to be added, modified, replaced, removed, or supported by different vendors throughout the lifecycle of the system to afford opportunities for enhanced competition and innovation while yielding—

''(i) significant cost and schedule savings; and

''(ii) increased interoperability.''

OPERATIONAL METRICS FOR JOINT INFORMATION ENVIRONMENT AND SUPPORTING ACTIVITIES

Pub. L. 113–291, div. A, title VIII, § 854, Dec. 19, 2014, 128 Stat. 3459, provided that:

''(a) GUIDANCE.—Not later than 180 days after the date of the enactment of this Act [Dec. 19, 2014], the Secretary of Defense, acting through the Chief Information Officer of the Department of Defense, shall issue guidance for measuring the operational effectiveness and efficiency of the Joint Information Environment within the military departments, Defense Agencies, and combatant commands. The guidance shall include a definition of specific metrics for data collection, and a requirement for each military department, Defense Agency, and combatant command to regularly collect and assess data on such operational effectiveness and efficiency and report the results to such Chief Information Officer on a regular basis.

''(b) BASELINE ARCHITECTURE.—The Chief Information Officer of the Department of Defense shall identify a baseline architecture for the Joint Information Environment by identifying and reporting to the Secretary of Defense any information technology programs or other investments that support that architecture.

''(c) JOINT INFORMATION ENVIRONMENT DEFINED.—In this section, the term 'Joint Information Environment' means the initiative of the Department of Defense to modernize the information technology networks and systems within the Department.''

SUPERVISION OF THE ACQUISITION OF CLOUD COMPUTING CAPABILITIES

Pub. L. 113–66, div. A, title IX, § 938, Dec. 26, 2013, 127 Stat. 835, provided that:

''(a) SUPERVISION.—

''(1) IN GENERAL.—The Secretary of Defense shall, acting through the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Under Secretary of Defense for Intelligence, the Chief Information Officer of the Department of Defense, and the Chairman of the Joint Requirements Oversight Council, supervise the following:

''(A) Review, development, modification, and approval of requirements for cloud computing solutions for data analysis and storage by the Armed Forces and the Defense Agencies, including requirements for cross-domain, enterprise-wide discovery and correlation of data stored in cloud and non-cloud computing databases, relational and non-relational databases, and hybrid databases.

''(B) Review, development, modification, approval, and implementation of plans for the competitive acquisition of cloud computing systems or services to meet requirements described in subparagraph (A), including plans for the transition from current computing systems to systems or services acquired.

''(C) Development and implementation of plans to ensure that the cloud systems or services acquired pursuant to subparagraph (B) are interoperable and universally accessible and usable through attribute-based access controls.

''(D) Integration of plans under subparagraphs (B) and (C) with enterprise-wide plans of the Armed Forces and the Department of Defense for the Joint Information Environment and the Defense Intelligence Information Environment.

''(2) DIRECTION.—The Secretary shall provide direction to the Armed Forces and the Defense Agencies on the matters covered by paragraph (1) by not later than March 15, 2014.

''(b) INTEGRATION WITH INTELLIGENCE COMMUNITY EFFORTS.—The Secretary shall coordinate with the Director of National Intelligence to ensure that activities under this section are integrated with the Intelligence Community Information Technology Enterprise in order to achieve interoperability, information sharing, and other efficiencies.

''(c) LIMITATION.—The requirements of subparagraphs (B), (C), and (D) of subsection (a)(1) shall not apply to a contract for the acquisition of cloud computing capabilities in an amount less than $1,000,000.

''(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to alter or affect the authorities or responsibilities of the Director of National Intelligence under section 102A of the National Security Act of 1947 (50 U.S.C. 3024).''

COMPETITION IN CONNECTION WITH DEPARTMENT OF DEFENSE TACTICAL DATA LINK SYSTEMS

Pub. L. 112–239, div. A, title IX, § 934, Jan. 2, 2013, 126 Stat. 1885, as amended by Pub. L. 113–66, div. A, title IX, § 931, Dec. 26, 2013, 127 Stat. 829, which provided that the upgrade, new deployment, or replacement of defense tactical data link systems should be open to competition, was repealed by Pub. L. 115–232, div. A, title VIII, § 812(b)(1), Aug. 13, 2018, 132 Stat. 1847.

DATA SERVERS AND CENTERS

Pub. L. 112–81, div. B, title XXVIII, § 2867, Dec. 31, 2011, 125 Stat. 1704, as amended by Pub. L. 112–239, div. B, title XXVIII, § 2853, Jan. 2, 2013, 126 Stat. 2161; Pub. L. 115–91, div. A, title X, § 1051(q)(3), Dec. 12, 2017, 131 Stat. 1565, 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).

''(3) REPORTS.—Not later than 30 days after the end of each calendar quarter, each Chief Information Officer of a component of the Department who grants an approval under paragraph (1) during such calendar quarter shall submit to the Chief Information Officer of the Department a report on the approval or approvals so granted during such calendar quarter.

''(b) PERFORMANCE PLAN FOR REDUCTION OF RESOURCES REQUIRED FOR DATA SERVERS AND CENTERS.—

''(1) COMPONENT PLANS.—

''(A) IN GENERAL.—Not later than January 15, 2012, the Secretaries of the military departments and the heads of the Defense Agencies shall each submit to the Chief Information Officer of the Department a plan for the department or agency concerned to achieve the following:

''(i) A reduction in the square feet of floor space devoted to information systems technologies, attendant support technologies, and operations within data centers.

''(ii) A reduction in the use of all utilities necessary to power and cool information systems technologies and data centers.

''(iii) An increase in multi-organizational utilization of data centers, information systems technologies, and associated resources.

''(iv) A reduction in the investment for capital infrastructure or equipment required to support data centers as measured in cost per megawatt of data storage.

''(v) A reduction in the number of commercial and government developed applications running on data servers and within data centers.

''(vi) A reduction in the number of government and vendor provided full-time equivalent personnel, and in the cost of labor, associated with the operation of data servers and data centers.

''(B) SPECIFICATION OF REQUIRED ELEMENTS.—The Chief Information Officer of the Department shall specify the particular performance standards and measures and implementation elements to be included in the plans submitted under this paragraph, including specific goals and schedules for achieving the matters specified in subparagraph (A).

''(2) DEFENSE-WIDE PLAN.—

''(A) IN GENERAL.—Not later than April 1, 2012, the Chief Information Officer of the Department shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a performance plan for a reduction in the resources required for data centers and information systems technologies Department-wide. The plan shall be based upon and incorporate appropriate elements of the plans submitted under paragraph (1).

''(B) ELEMENTS.—The performance plan required under this paragraph shall include the following:

''(i) A Department-wide performance plan for achieving the matters specified in paragraph (1)(A), including performance standards and measures for data centers and information systems technologies, goals and schedules for achieving such matters, and an estimate of cost savings anticipated through implementation of the plan.

''(ii) A Department-wide strategy for each of the following:

''(I) Desktop, laptop, and mobile device virtualization.

''(II) Transitioning to cloud computing.

''(III) Migration of Defense data and government-provided services from Department-owned and operated data centers to cloud computing services generally available within the private sector that provide a better capability at a lower cost with the same or greater degree of security.

''(IV) Utilization of private sector-managed security services for data centers and cloud computing services.

''(V) A finite set of metrics to accurately and transparently report on data center infrastructure (space, power and cooling): age, cost, capacity, usage, energy efficiency and utilization, accompanied with the aggregate data for each data center site in use by the Department in excess of 100 kilowatts of information technology power demand.

''(VI) Transitioning to just-in-time delivery of Department-owned data center infrastructure (space, power and cooling) through use of modular data center technology and integrated data center infrastructure management software.

''(3) RESPONSIBILITY.—The Chief Information Officer of the Department shall discharge the responsibility for establishing performance standards and measures for data centers and information systems technologies for purposes of this subsection. Such responsibility may not be delegated.

''(c) EXCEPTIONS.—

''(1) INTELLIGENCE COMPONENTS.—The Chief Information Officer of the Department and the Chief Information Officer of the Intelligence Community may jointly exempt from the applicability of this section such intelligence components of the Department of Defense (and the programs and activities thereof) that are funded through the National Intelligence Program (NIP) as the Chief Information Officers consider appropriate.

''(2) RESEARCH, DEVELOPMENT, TEST, AND EVALUATION PROGRAMS.—The Chief Information Officer of the Department may exempt from the applicability of this section research, development, test, and evaluation programs that use authorization of appropriations for the High Performance Computing Modernization Program (Program Element 0603461A) if the Chief Information Officer determines that the exemption is in the best interest of national security.''

DEMONSTRATION AND PILOT PROJECTS ON CYBERSECURITY

Pub. L. 111–383, div. A, title II, § 215, Jan. 7, 2011, 124 Stat. 4165, provided that:

''(a) DEMONSTRATION PROJECTS ON PROCESSES FOR APPLICATION OF COMMERCIAL TECHNOLOGIES TO CYBERSECURITY REQUIREMENTS.—

''(1) PROJECTS REQUIRED.—The Secretary of Defense and the Secretaries of the military departments shall jointly carry out demonstration projects to assess the feasibility and advisability of using various business models and processes to rapidly and effectively identify innovative commercial technologies and apply such technologies to Department of Defense and other cybersecurity requirements.

''(2) SCOPE OF PROJECTS.—Any demonstration project under paragraph (1) shall be carried out in such a manner as to contribute to the cyber policy review of the President and the Comprehensive National Cybersecurity Initiative.

''(b) PILOT PROGRAMS ON CYBERSECURITY REQUIRED.—The Secretary of Defense shall support or conduct pilot programs on cybersecurity with respect to the following areas:

''(1) Threat sensing and warning for information networks worldwide.

''(2) Managed security services for cybersecurity within the defense industrial base, military departments, and combatant commands.

''(3) Use of private processes and infrastructure to address threats, problems, vulnerabilities, or opportunities in cybersecurity.

''(4) Processes for securing the global supply chain.

''(5) Processes for threat sensing and security of cloud computing infrastructure.

''(c) REPORTS.—

''(1) REPORTS REQUIRED.—Not later than 240 days after the date of the enactment of this Act [Jan. 7, 2011], and annually thereafter at or about the time of the submittal to Congress of the budget of the President for a fiscal year (as submitted pursuant to section 1105(a) of title 31, United States Code), the Secretary of Defense shall, in coordination with the Secretary of Homeland Security, submit to Congress a report on any demonstration projects carried out under subsection (a), and on the pilot projects carried out under subsection (b), during the preceding year.

''(2) ELEMENTS.—Each report under this subsection shall include the following:

''(A) A description and assessment of any activities under the demonstration projects and pilot projects referred to in paragraph (1) during the preceding year.

''(B) For the pilot projects supported or conducted under subsection (b)(2)—

''(i) a quantitative and qualitative assessment of the extent to which managed security services covered by the pilot project could provide effective and affordable cybersecurity capabilities for components of the Department of Defense and for entities in the defense industrial base, and an assessment whether such services could be expanded rapidly to a large scale without exceeding the ability of the Federal Government to manage such expansion; and

''(ii) an assessment of whether managed security services are compatible with the cybersecurity strategy of the Department of Defense with respect to conducting an active, in-depth defense under the direction of United States Cyber Command.

''(C) For the pilot projects supported or conducted under subsection (b)(3)—

''(i) a description of any performance metrics established for purposes of the pilot project, and a description of any processes developed for purposes of accountability and governance under any partnership under the pilot project; and

''(ii) an assessment of the role a partnership such as a partnership under the pilot project would play in the acquisition of cyberspace capabilities by the Department of Defense, including a role with respect to the development and approval of requirements, approval and oversight of acquiring capabilities, test and evaluation of new capabilities, and budgeting for new capabilities.

''(D) For the pilot projects supported or conducted under subsection (b)(4)—

''(i) a framework and taxonomy for evaluating practices that secure the global supply chain, as well as practices for securely operating in an uncertain or compromised supply chain;

''(ii) an assessment of the viability of applying commercial practices for securing the global supply chain; and

''(iii) an assessment of the viability of applying commercial practices for securely operating in an uncertain or compromised supply chain.

''(E) For the pilot projects supported or conducted under subsection (b)(5)—

''(i) an assessment of the capabilities of Federal Government providers to offer secure cloud computing environments; and

''(ii) an assessment of the capabilities of commercial providers to offer secure cloud computing environments to the Federal Government.

''(3) FORM.—Each report under this subsection shall be submitted in unclassified form, but may include a classified annex.''

IMPLEMENTATION OF NEW ACQUISITION PROCESS FOR INFORMATION TECHNOLOGY SYSTEMS

Pub. L. 111–84, div. A, title VIII, § 804, Oct. 28, 2009, 123 Stat. 2402, which provided for development and implementation of a new acquisition process for information technology systems, was repealed by Pub. L. 115–232, div. A, title VIII, § 812(b)(2), Aug. 13, 2018, 132 Stat. 1848.

CLEARINGHOUSE FOR RAPID IDENTIFICATION AND DISSEMINATION OF COMMERCIAL INFORMATION TECHNOLOGIES

Pub. L. 110–181, div. A, title VIII, § 881, Jan. 28, 2008, 122 Stat. 262, provided that:

''(a) REQUIREMENT TO ESTABLISH CLEARINGHOUSE.—Not later than 180 days after the date of the enactment of this Act [Jan. 28, 2008], the Secretary of Defense, acting through the Assistant Secretary of Defense for Networks and Information Integration, shall establish a clearinghouse for identifying, assessing, and disseminating knowledge about readily available information technologies (with an emphasis on commercial off-the-shelf information technologies) that could support the warfighting mission of the Department of Defense.

''(b) RESPONSIBILITIES.—The clearinghouse established pursuant to subsection (a) shall be responsible for the following:

''(1) Developing a process to rapidly assess and set priorities and needs for significant information technology needs of the Department of Defense that could be met by commercial technologies, including a process for—

''(A) aligning priorities and needs with the requirements of the commanders of the combatant command; and

''(B) proposing recommendations to the commanders of the combatant command of feasible technical solutions for further evaluation.

''(2) Identifying and assessing emerging commercial technologies (including commercial off-the-shelf technologies) that could support the warfighting mission of the Department of Defense, including the priorities and needs identified pursuant to paragraph (1).

''(3) Disseminating information about commercial technologies identified pursuant to paragraph (2) to commanders of combatant commands and other potential users of such technologies.

''(4) Identifying gaps in commercial technologies and working to stimulate investment in research and development in the public and private sectors to address those gaps.

''(5) Enhancing internal data and communications systems of the Department of Defense for sharing and retaining information regarding commercial technology priorities and needs, technologies available to meet such priorities and needs, and ongoing research and development directed toward gaps in such technologies.

''(6) Developing mechanisms, including web-based mechanisms, to facilitate communications with industry regarding the priorities and needs of the Department of Defense identified pursuant to paragraph (1) and commercial technologies available to address such priorities and needs.

''(7) Assisting in the development of guides to help small information technology companies with promising technologies to understand and navigate the funding and acquisition processes of the Department of Defense.

''(8) Developing methods to measure how well processes developed by the clearinghouse are being utilized and to collect data on an ongoing basis to assess the benefits of commercial technologies that are procured on the recommendation of the clearinghouse.

''(c) PERSONNEL.—The Secretary of Defense, acting through the Assistant Secretary of Defense for Net-

works and Information Integration, shall provide for the hiring and support of employees (including detailees from other components of the Department of Defense and from other Federal departments or agencies) to assist in identifying, assessing, and disseminating information regarding commercial technologies under this section.

''(d) REPORT TO CONGRESS.—Not later than one year after the date of the enactment of this Act [Jan. 28, 2008], the Secretary of Defense 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 implementation of this section.''

§ 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.)

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 meet the requirements of section 3534 and 3535 of title 44, United States Code.'' could not be executed. See above par.

Subsec. (c). Pub. L. 107–347, § 301(c)(1)(B)(iii), inserted '', including through compliance with subchapter III of chapter 35 of title 44'' after ''infrastructure'' in introductory provisions.

Pub. L. 107–296, § 1001(c)(1)(B)(iii), inserted '', including through compliance with subtitle II of chapter 35 of title 44'' after ''infrastructure'' in introductory provisions.

2000—Subsec. (b). Pub. L. 106–398, § 1 [[div. A], title X, § 1063(a)], substituted ''OBJECTIVES AND MINIMUM REQUIREMENTS'' for ''OBJECTIVES OF THE PROGRAM'' in heading, designated existing provisions as par. (1), and added par. (2).

Subsec. (e)(7). Pub. L. 106–398, § 1 [[div. A], title X, § 1063(b)], added par. (7).

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as