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

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

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

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

CONTINUOUS MONITORING OF DEPARTMENT OF DEFENSE INFORMATION SYSTEMS FOR CYBERSECURITY

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

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

''(1) The continuous prioritization of the policies, principles, standards, and guidelines developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) based upon the evolving threat of information security incidents with respect to national security systems, the vulnerability of such systems to such incidents, and the consequences of information security incidents involving such systems.

''(2) The automation of continuous monitoring of the effectiveness of the information security policies, procedures, and practices within the information infrastructure of the Department of Defense, and the compliance of that infrastructure with such policies, procedures, and practices, including automation of—

''(A) management, operational, and technical controls of every information system identified in the inventory required under section 3505(c) of title 44, United States Code; and

''(B) management, operational, and technical controls relied on for evaluations under [former] section 3545 of title 44, United States Code [see now 44 U.S.C. 3555].

''(b) DEFINITIONS.—In this section:

''(1) The term 'information security incident' means an occurrence that—

''(A) actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information such system processes, stores, or transmits; or

''(B) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies with respect to an information system.

''(2) The term 'information infrastructure' means the underlying framework, equipment, and software that an information system and related assets rely on to process, transmit, receive, or store information electronically.

''(3) The term 'national security system' has the meaning given that term in [former] section 3542(b)(2) of title 44, United States Code [see now 44 U.S.C. 3552(b)(6)].''

§ 2223a. Information technology acquisition planning and oversight requirements

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

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

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

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

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

(B) continuous process improvement of such programs; and

(C) achievement of program and investment outcomes;

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

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

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

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

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

GUIDANCE ON ACQUISITION OF BUSINESS SYSTEMS

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

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

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

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

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

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

''(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, provided that:

''(a) COMPETITION IN CONNECTION WITH TACTICAL DATA LINK SYSTEMS.—Not later than December 1, 2013, the Under Secretary of Defense for Acquisition, Technology, and Logistics shall—

''(1) develop an inventory of all tactical data link systems in use and in development in the Department of Defense, including interfaces and waveforms and an assessment of vulnerabilities to such systems in anti-access or area-denial environments;

''(2) conduct an analysis of each data link system contained in the inventory under paragraph (1) to determine whether—

''(A) the upgrade, new deployment, or replacement of such system should be open to competition; or

''(B) the data link should be converted to an open architecture, or a different data link standard should be adopted to enable such competition;

''(3) for each data link system for which competition is determined advisable under subparagraph (A) or (B) of paragraph (2), develop a plan to achieve such competition, including a plan to address any policy, legal, programmatic, or technical barriers to such competition; and

''(4) for each data link system for which competition is determined not advisable under paragraph (2), prepare an explanation for such determination.

''(b) EARLIER ACTIONS.—If the Under Secretary completes any portion of the plan described in subsection (a)(3) before December 1, 2013, the Secretary may commence action on such portion of the plan upon completion of such portion, including publication of such portion of the plan.

''(c) REPORT.—At the same time the budget of the President for fiscal year 2015 is submitted to Congress pursuant to section 1105(a) of title 31, United States Code, the Under 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 plans described in paragraph (3) of subsection (a), including any explanation prepared under paragraph (4) of such subsection.''

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, 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.

''(d) REPORTS ON COST SAVINGS.—

''(1) IN GENERAL.—Not later than March 1 of each fiscal year, and ending in fiscal year 2016, the Chief Information Officer of the Department shall submit to the appropriate committees of Congress a report on the cost savings, cost reductions, cost avoidances, and performance gains achieved, and anticipated to be achieved, as of the date of such report as a result of activities undertaken under this section.

''(2) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this subsection, the term 'appropriate committees of Congress' means—

''(A) the Committee on Armed Services, the Committee on Appropriations, and the Select Committee on Intelligence of the Senate; and

''(B) the Committee on Armed Services, the Committee on Appropriations, and the Permanent Select Committee on Intelligence of the House of Representatives.''

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, provided that:

''(a) NEW ACQUISITION PROCESS REQUIRED.—The Secretary of Defense shall develop and implement a new acquisition process for information technology systems. The acquisition process developed and implemented pursuant to this subsection shall, to the extent determined appropriate by the Secretary—

''(1) be based on the recommendations in chapter 6 of the March 2009 report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology; and

''(2) be designed to include—

''(A) early and continual involvement of the user;

''(B) multiple, rapidly executed increments or releases of capability;

''(C) early, successive prototyping to support an evolutionary approach; and

''(D) a modular, open-systems approach.

''(b) REPORT TO CONGRESS.—Not later than 270 days after the date of the enactment of this Act [Oct. 28, 2009], the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report on the new acquisition process developed pursuant to subsection (a). The report required by this subsection shall, at a minimum—

''(1) describe the new acquisition process;

''(2) provide an explanation for any decision by the Secretary to deviate from the criteria established for such process in paragraphs (1) and (2) of subsection (a);

''(3) provide a schedule for the implementation of the new acquisition process;

''(4) identify the categories of information technology acquisitions to which such process will apply; and

''(5) include the Secretary's recommendations for any legislation that may be required to implement the new acquisition process.''

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 Networks 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,