''(3) Mechanisms for protection against compromise of information systems through the supply chain or cyber attack by acquiring and improving automated tools for—

''(A) assuring the security of software and software applications during software development;

''(B) detecting vulnerabilities during testing of software; and

''(C) detecting intrusions during real-time monitoring of software applications.

''(4) Mechanisms providing the Department of Defense with the capabilities—

''(A) to monitor systems and applications in order to detect and defeat attempts to penetrate or disable such systems and applications; and

''(B) to ensure that such monitoring capabilities are integrated into the Department of Defense system of cyber defense-in-depth capabilities.

''(5) An update to Committee for National Security Systems Instruction No. 4009, entitled 'National Information Assurance Glossary', to include a standard definition for software security assurance.

''(6) Either—

''(A) mechanisms to ensure that vulnerable Mission Assurance Category III information systems, if penetrated, cannot be used as a foundation for penetration of protected covered systems, and means for assessing the effectiveness of such mechanisms; or

''(B) plans to address critical vulnerabilities in Mission Assurance Category III information systems to prevent their use for intrusions of Mission Assurance Category I systems and Mission Assurance Category II systems.

''(7) A funding mechanism for remediation of critical software assurance vulnerabilities in legacy systems.

''(d) REPORT.—Not later than October 1, 2011, 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 strategy required by subsection (a). The report shall include the following:

''(1) A description of the current status of the strategy required by subsection (a) and of the implementation of the strategy, including a description of the role of the strategy in the risk management by the Department regarding the supply chain and in operational planning for cyber security.

''(2) A description of the risks, if any, that the Department will accept in the strategy due to limitations on funds or other applicable constraints.''

INSTITUTE FOR DEFENSE COMPUTER SECURITY AND INFORMATION PROTECTION

Pub. L. 106–398, § 1 [[div. A], title IX, § 921], Oct. 30, 2000, 114 Stat. 1654, 1654A–233, provided that:

''(a) ESTABLISHMENT.—The Secretary of Defense shall establish an Institute for Defense Computer Security and Information Protection.

''(b) MISSION.—The Secretary shall require the institute—

''(1) to conduct research and technology development that is relevant to foreseeable computer and network security requirements and information assurance requirements of the Department of Defense with a principal focus on areas not being carried out by other organizations in the private or public sector; and

''(2) to facilitate the exchange of information regarding cyberthreats, technology, tools, and other relevant issues.

''(c) CONTRACTOR OPERATION.—The Secretary shall enter into a contract with a not-for-profit entity, or a consortium of not-for-profit entities, to organize and operate the institute. The Secretary shall use competitive procedures for the selection of the contractor to the extent determined necessary by the Secretary.

''(d) FUNDING.—Of the amount authorized to be appropriated by section 301(5) [114 Stat. 1654A–52], $5,000,000 shall be available for the Institute for Defense Computer Security and Information Protection.

''(e) REPORT.—Not later than April 1, 2001, the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] the Secretary's plan for implementing this section.''

§ 2224a. Information security: continued applicability of expiring Governmentwide requirements to the Department of Defense

(a) IN GENERAL.—The provisions of subchapter II[1] of chapter 35 of title 44 shall continue to apply through September 30, 2004, with respect to the Department of Defense, notwithstanding the expiration of authority under section 3536[1] of such title.

(b) RESPONSIBILITIES.—In administering the provisions of subchapter II[1] of chapter 35 of title 44 with respect to the Department of Defense after the expiration of authority under section 3536[1] of such title, the Secretary of Defense shall perform the duties set forth in that subchapter for the Director of the Office of Management and Budget.

(Added Pub. L. 107–314, div. A, title X, § 1052(b)(1), Dec. 2, 2002, 116 Stat. 2648.)

REFERENCES IN TEXT

Provisions relating to the expiration of authority of subchapter II of chapter 35 of title 44, referred to in text, did not appear in section 3536 of title 44 subsequent to the general revision of subchapter II by Pub. L. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2259. Subchapter II, as revised by Pub. L. 107–296, was repealed and a new subchapter II enacted by Pub. L. 113–283, § 2(a), Dec. 18, 2014, 128 Stat. 3073.

§ 2225. Information technology purchases: tracking and management

(a) COLLECTION OF DATA REQUIRED.—To improve tracking and management of information technology products and services by the Department of Defense, the Secretary of Defense shall provide for the collection of the data described in subsection (b) for each purchase of such products or services made by a military department or Defense Agency in excess of the simplified acquisition threshold, regardless of whether such a purchase is made in the form of a contract, task order, delivery order, military interdepartmental purchase request, or any other form of interagency agreement.

(b) DATA TO BE COLLECTED.—The data required to be collected under subsection (a) includes the following:

(1) The products or services purchased.

(2) Whether the products or services are categorized as commercially available off-the-shelf items, other commercial items, nondevelopmental items other than commercial items, other noncommercial items, or services.

(3) The total dollar amount of the purchase.

(4) The form of contracting action used to make the purchase.

(5) In the case of a purchase made through an agency other than the Department of Defense—

[1] See References in Text note below.

(A) the agency through which the purchase is made; and

(B) the reasons for making the purchase through that agency.

(6) The type of pricing used to make the purchase (whether fixed price or another type of pricing).

(7) The extent of competition provided in making the purchase.

(8) A statement regarding whether the purchase was made from—

(A) a small business concern;

(B) a small business concern owned and controlled by socially and economically disadvantaged individuals; or

(C) a small business concern owned and controlled by women.

(9) A statement regarding whether the purchase was made in compliance with the planning requirements under sections 11312 and 11313 of title 40.

(c) RESPONSIBILITY TO ENSURE FAIRNESS OF CERTAIN PRICES.—The head of each contracting activity in the Department of Defense shall have responsibility for ensuring the fairness and reasonableness of unit prices paid by the contracting activity for information technology products and services that are frequently purchased commercially available off-the-shelf items.

(d) LIMITATION ON CERTAIN PURCHASES.—No purchase of information technology products or services in excess of the simplified acquisition threshold shall be made for the Department of Defense from a Federal agency outside the Department of Defense unless—

(1) the purchase data is collected in accordance with subsection (a); or

(2)(A) in the case of a purchase by a Defense Agency, the purchase is approved by the Under Secretary of Defense for Acquisition, Technology, and Logistics; or

(B) in the case of a purchase by a military department, the purchase is approved by the senior procurement executive of the military department.

(e) ANNUAL REPORT.—Not later than March 15 of each year, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report containing a summary of the data collected in accordance with subsection (a).

(f) DEFINITIONS.—In this section:

(1) The term ''senior procurement executive'', with respect to a military department, means the official designated as the senior procurement executive for the military department for the purposes of section 1702(c) of title 41.

(2) The term ''simplified acquisition threshold'' has the meaning given the term in section 134 of title 41.

(3) The term ''small business concern'' means a business concern that meets the applicable size standards prescribed pursuant to section 3(a) of the Small Business Act (15 U.S.C. 632(a)).

(4) The term ''small business concern owned and controlled by socially and economically disadvantaged individuals'' has the meaning given that term in section 8(d)(3)(C) of the Small Business Act (15 U.S.C. 637(d)(3)(C)).

(5) The term ''small business concern owned and controlled by women'' has the meaning given that term in section 8(d)(3)(D) of the Small Business Act (15 U.S.C. 637(d)(3)(D)).

(Added Pub. L. 106–398, §1 [[div. A], title VIII, §812(a)(1)], Oct. 30, 2000, 114 Stat. 1654, 1654A–212; amended Pub. L. 108–178, §4(b)(2), Dec. 15, 2003, 117 Stat. 2640; Pub. L. 109–364, div. A, title X, §1071(a)(2), Oct. 17, 2006, 120 Stat. 2398; Pub. L. 111–350, §5(b)(6), Jan. 4, 2011, 124 Stat. 3842.)

AMENDMENTS

2011—Subsec. (f)(1). Pub. L. 111–350, §5(b)(6)(A), substituted ''section 1702(c) of title 41'' for ''section 16(c) of the Office of Federal Procurement Policy Act (41 U.S.C. 414(c))''.

Subsec. (f)(2). Pub. L. 111–350, §5(b)(6)(B), substituted ''section 134 of title 41'' for ''section 4(11) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(11))''.

2006—Subsec. (f)(1). Pub. L. 109–364 substituted ''section 16(c) of the Office of Federal Procurement Policy Act (41 U.S.C. 414(c))'' for ''section 16(3) of the Office of Federal Procurement Policy Act (41 U.S.C. 414(3))''.

2003—Subsec. (b)(9). Pub. L. 108–178 substituted ''sections 11312 and 11313 of title 40'' for ''sections 5122 and 5123 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1422, 1423)''.

EFFECTIVE DATE OF 2003 AMENDMENT

Amendment by Pub. L. 108–178 effective Aug. 21, 2002, see section 5 of Pub. L. 108–178, set out as a note under section 5334 of Title 5, Government Organization and Employees.

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).''

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.''

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.''

TIME FOR IMPLEMENTATION; APPLICABILITY

Pub. L. 106–398, §1 [[div. A], title VIII, §812(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–214, provided that:

''(1) The Secretary of Defense shall collect data as required under section 2225 of title 10, United States Code (as added by subsection (a)) for all contractual actions covered by such section entered into on or after the date that is one year after the date of the enactment of this Act [Oct. 30, 2000].

''(2) Subsection (d) of such section shall apply with respect to purchases described in that subsection for which solicitations of offers are issued on or after the date that is one year after the date of the enactment of this Act.''

GAO REPORT

Pub. L. 106–398, §1 [[div. A], title VIII, §812(c)], Oct. 30, 2000, 114 Stat. 1654, 1654A–214, directed the Comptroller General to submit to committees of Congress a report on the collection of data under this section not later than 15 months after Oct. 30, 2000.

§ 2226. Contracted property and services: prompt payment of vouchers

(a) REQUIREMENT.—Of the contract vouchers that are received by the Defense Finance and