''(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.''

§ 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 an Effective Date note under section 101 of Title 6, Domestic Security.

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, § 1065] of

Pub. L. 106–398, set out as an Effective Date note under section 3531 of Title 44, Public Printing and Documents.

AUTHORITIES, CAPABILITIES, AND OVERSIGHT OF THE UNITED STATES CYBER COMMAND

Pub. L. 113–66, div. A, title IX, §932, Dec. 26, 2013, 127 Stat. 829, provided that:

''(a) PROVISION OF CERTAIN OPERATIONAL CAPABILITIES.—The Secretary of Defense shall take such actions as the Secretary considers appropriate to provide the United States Cyber Command operational military units with infrastructure and equipment enabling access to the Internet and other types of networks to permit the United States Cyber Command to conduct the peacetime and wartime missions of the Command.

''(b) CYBER RANGES.—

''(1) IN GENERAL.—The Secretary shall review existing cyber ranges and adapt one or more such ranges, as necessary, to support training and exercises of cyber units that are assigned to execute offensive military cyber operations.

''(2) ELEMENTS.—Each range adapted under paragraph (1) shall have the capability to support offensive military operations against targets that—

''(A) have not been previously identified and prepared for attack; and

''(B) must be compromised or neutralized immediately without regard to whether the adversary can detect or attribute the attack.

''(c) PRINCIPAL ADVISOR ON MILITARY CYBER FORCE MATTERS.—

''(1) DESIGNATION.—The Secretary shall designate, from among the personnel of the Office of the Under Secretary of Defense for Policy, a Principal Cyber Advisor to act as the principal advisor to the Secretary on military cyber forces and activities. The Secretary may only designate an official under this paragraph if such official was appointed to the position in which such official serves by and with the advice and consent of the Senate.

''(2) RESPONSIBILITIES.—The Principal Cyber Advisor shall be responsible for the following:

''(A) Overall supervision of cyber activities related to offensive missions, defense of the United States, and defense of Department of Defense networks, including oversight of policy and operational considerations, resources, personnel, and acquisition and technology.

''(B) Such other matters relating to offensive military cyber forces as the Secretary shall specify for purposes of this subsection.

''(3) CROSS-FUNCTIONAL TEAM.—The Principal Cyber Advisor shall—

''(A) integrate the cyber expertise and perspectives of appropriate organizations within the Office of the Secretary of Defense, Joint Staff, military departments, Defense Agencies, and combatant commands, by establishing and maintaining a full-time cross-functional team of subject matter experts from those organizations; and

''(B) select team members, and designate a team leader, from among those personnel nominated by the heads of such organizations.

''(d) TRAINING OF CYBER PERSONNEL.—The Secretary shall establish and maintain training capabilities and facilities in the Armed Forces and, as the Secretary considers appropriate, at the United States Cyber Command, to support the needs of the Armed Forces and the United States Cyber Command for personnel who are assigned offensive and defensive cyber missions in the Department of Defense.''

JOINT FEDERATED CENTERS FOR TRUSTED DEFENSE SYSTEMS FOR THE DEPARTMENT OF DEFENSE

Pub. L. 113–66, div. A, title IX, §937, Dec. 26, 2013, 127 Stat. 834, provided that:

''(a) FEDERATION REQUIRED.—

''(1) IN GENERAL.—The Secretary of Defense shall provide for the establishment of a joint federation of capabilities to support the trusted defense system needs of the Department of Defense (in this section referred to as the 'federation').

''(2) PURPOSE.—The purpose of the federation shall be to serve as a joint, Department-wide federation of capabilities to support the trusted defense system needs of the Department to ensure security in the software and hardware developed, acquired, maintained, and used by the Department, pursuant to the trusted defense systems strategy of the Department and supporting policies related to software assurance and supply chain risk management.

''(b) DISCHARGE OF ESTABLISHMENT.—In providing for the establishment of the federation, the Secretary shall consider whether the purpose of the federation can be met by existing centers in the Department. If the Department determines that there are capabilities gaps that cannot be satisfied by existing centers, the Department shall devise a strategy for creating and providing resources for such capabilities to fill such gaps.

''(c) CHARTER.—Not later than 180 days after the date of the enactment of this Act [Dec. 26, 2013], the Secretary shall issue a charter for the federation. The charter shall—

''(1) be established pursuant to the trusted defense systems strategy of the Department and supporting policies related to software assurance and supply chain risk management; and

''(2) set forth—

''(A) the role of the federation in supporting program offices in implementing the trusted defense systems strategy of the Department;

''(B) the software and hardware assurance expertise and capabilities of the federation, including policies, standards, requirements, best practices, contracting, training, and testing;

''(C) the requirements for the discharge by the federation, in coordination with the Center for Assured Software of the National Security Agency, of a program of research and development to improve automated software code vulnerability analysis and testing tools;

''(D) the requirements for the federation to procure, manage, and distribute enterprise licenses for automated software vulnerability analysis tools; and

''(E) the requirements for the discharge by the federation, in coordination with the Defense Microelectronics Activity, of a program of research and development to improve hardware vulnerability, testing, and protection tools.

''(d) REPORT.—The Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives], at the time of the submittal to Congress of the budget of the President for fiscal year 2016 pursuant to section 1105 of title 31, United States Code, a report on the funding and management of the federation. The report shall set forth such recommendations as the Secretary considers appropriate regarding the optimal placement of the federation within the organizational structure of the Department, including responsibility for the funding and management of the federation.''

IMPROVEMENTS IN ASSURANCE OF COMPUTER SOFTWARE PROCURED BY THE DEPARTMENT OF DEFENSE

Pub. L. 112–239, div. A, title IX, §933, Jan. 2, 2013, 126 Stat. 1884, provided that:

''(a) BASELINE SOFTWARE ASSURANCE POLICY.—The Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the Chief Information Officer of the Department of Defense, shall develop and implement a baseline software assurance policy for the entire lifecycle of covered systems. Such policy shall be included as part of the strategy for trusted defense systems of the Department of Defense.

''(b) POLICY ELEMENTS.—The baseline software assurance policy under subsection (a) shall—

''(1) require use of appropriate automated vulnerability analysis tools in computer software code dur-

ing the entire lifecycle of a covered system, including during development, operational testing, operations and sustainment phases, and retirement;

''(2) require covered systems to identify and prioritize security vulnerabilities and, based on risk, determine appropriate remediation strategies for such security vulnerabilities;

''(3) ensure such remediation strategies are translated into contract requirements and evaluated during source selection;

''(4) promote best practices and standards to achieve software security, assurance, and quality; and

''(5) support competition and allow flexibility and compatibility with current or emerging software methodologies.

''(c) VERIFICATION OF EFFECTIVE IMPLEMENTATION.—The Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the Chief Information Officer of the Department of Defense, shall—

''(1) collect data on implementation of the policy developed under subsection (a) and measure the effectiveness of such policy, including the particular elements required under subsection (b); and

''(2) identify and promote best practices, tools, and standards for developing and validating assured software for the Department of Defense.

''(d) BRIEFING ON ADDITIONAL MEANS OF IMPROVING SOFTWARE ASSURANCE.—Not later than one year after the date of the enactment of this Act [Jan. 2, 2013], the Under Secretary for Acquisition, Technology, and Logistics shall, in coordination with the Chief Information Officer of the Department of Defense, provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the following:

''(1) A research and development strategy to advance capabilities in software assurance and vulnerability detection.

''(2) The state-of-the-art of software assurance analysis and test.

''(3) How the Department might hold contractors liable for software defects or vulnerabilities.

''(e) DEFINITIONS.—In this section:

''(1) COVERED SYSTEM.—The term 'covered system' means any Department of Defense critical information, business, or weapons system that is—

''(A) a major system, as that term is defined in section 2302(5) of title 10, United States Code;

''(B) a national security system, as that term is defined in section 3542(b)(2) of title 44, United States Code; or

''(C) a Department of Defense information system categorized as Mission Assurance Category I in Department of Defense Directive 8500.01E that is funded by the Department of Defense.

''(2) SOFTWARE ASSURANCE.—The term 'software assurance' means the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the life cycle.''

REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS

Pub. L. 112–239, div. A, title IX, §941, Jan. 2, 2013, 126 Stat. 1889, provided that:

''(a) PROCEDURES FOR REPORTING PENETRATIONS.—The Secretary of Defense shall establish procedures that require each cleared defense contractor to report to a component of the Department of Defense designated by the Secretary for purposes of such procedures when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.

''(b) NETWORKS AND INFORMATION SYSTEMS SUBJECT TO REPORTING.—

''(1) CRITERIA.—The Secretary of Defense shall designate a senior official to, in consultation with the officials specified in paragraph (2), establish criteria for covered networks to be subject to the procedures for reporting system penetrations under subsection (a).

''(2) OFFICIALS.—The officials specified in this subsection are the following:

''(A) The Under Secretary of Defense for Policy.

''(B) The Under Secretary of Defense for Acquisition, Technology, and Logistics.

''(C) The Under Secretary of Defense for Intelligence.

''(D) The Chief Information Officer of the Department of Defense.

''(E) The Commander of the United States Cyber Command.

''(c) PROCEDURE REQUIREMENTS.—

''(1) RAPID REPORTING.—The procedures established pursuant to subsection (a) shall require each cleared defense contractor to rapidly report to a component of the Department of Defense designated pursuant to subsection (a) of each successful penetration of the network or information systems of such contractor that meet the criteria established pursuant to subsection (b). Each such report shall include the following:

''(A) A description of the technique or method used in such penetration.

''(B) A sample of the malicious software, if discovered and isolated by the contractor, involved in such penetration.

''(C) A summary of information created by or for the Department in connection with any Department program that has been potentially compromised due to such penetration.

''(2) ACCESS TO EQUIPMENT AND INFORMATION BY DEPARTMENT OF DEFENSE PERSONNEL.—The procedures established pursuant to subsection (a) shall—

''(A) include mechanisms for Department of Defense personnel to, upon request, obtain access to equipment or information of a cleared defense contractor necessary to conduct forensic analysis in addition to any analysis conducted by such contractor;

''(B) provide that a cleared defense contractor is only required to provide access to equipment or information as described in subparagraph (A) to determine whether information created by or for the Department in connection with any Department program was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated; and

''(C) provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person.

''(3) LIMITATION ON DISSEMINATION OF CERTAIN INFORMATION.—The procedures established pursuant to subsection (a) shall prohibit the dissemination outside the Department of Defense of information obtained or derived through such procedures that is not created by or for the Department except with the approval of the contractor providing such information.

''(d) ISSUANCE OF PROCEDURES AND ESTABLISHMENT OF CRITERIA.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act [Jan. 2, 2013]—

''(A) the Secretary of Defense shall establish the procedures required under subsection (a); and

''(B) the senior official designated under subsection (b)(1) shall establish the criteria required under such subsection.

''(2) APPLICABILITY DATE.—The requirements of this section shall apply on the date on which the Secretary of Defense establishes the procedures required under this section.

''(e) DEFINITIONS.—In this section:

''(1) CLEARED DEFENSE CONTRACTOR.—The term 'cleared defense contractor' means a private entity

granted clearance by the Department of Defense to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the Department of Defense.

''(2) COVERED NETWORK.—The term 'covered network' means a network or information system of a cleared defense contractor that contains or processes information created by or for the Department of Defense with respect to which such contractor is required to apply enhanced protection.''

INSIDER THREAT DETECTION

Pub. L. 112–81, div. A, title IX, §922, Dec. 31, 2011, 125 Stat. 1537, provided that:

''(a) PROGRAM REQUIRED.—The Secretary of Defense shall establish a program for information sharing protection and insider threat mitigation for the information systems of the Department of Defense to detect unauthorized access to, use of, or transmission of classified or controlled unclassified information.

''(b) ELEMENTS.—The program established under subsection (a) shall include the following:

''(1) Technology solutions for deployment within the Department of Defense that allow for centralized monitoring and detection of unauthorized activities, including—

''(A) monitoring the use of external ports and read and write capability controls;

''(B) disabling the removable media ports of computers physically or electronically;

''(C) electronic auditing and reporting of unusual and unauthorized user activities;

''(D) using data-loss prevention and data-rights management technology to prevent the unauthorized export of information from a network or to render such information unusable in the event of the unauthorized export of such information;

''(E) a roles-based access certification system;

''(F) cross-domain guards for transfers of information between different networks; and

''(G) patch management for software and security updates.

''(2) Policies and procedures to support such program, including special consideration for policies and procedures related to international and interagency partners and activities in support of ongoing operations in areas of hostilities.

''(3) A governance structure and process that integrates information security and sharing technologies with the policies and procedures referred to in paragraph (2). Such structure and process shall include—

''(A) coordination with the existing security clearance and suitability review process;

''(B) coordination of existing anomaly detection techniques, including those used in counterintelligence investigation or personnel screening activities; and

''(C) updating and expediting of the classification review and marking process.

''(4) A continuing analysis of—

''(A) gaps in security measures under the program; and

''(B) technology, policies, and processes needed to increase the capability of the program beyond the initially established full operating capability to address such gaps.

''(5) A baseline analysis framework that includes measures of performance and effectiveness.

''(6) A plan for how to ensure related security measures are put in place for other departments or agencies with access to Department of Defense networks.

''(7) A plan for enforcement to ensure that the program is being applied and implemented on a uniform and consistent basis.

''(c) OPERATING CAPABILITY.—The Secretary shall ensure the program established under subsection (a)—

''(1) achieves initial operating capability not later than October 1, 2012; and

''(2) achieves full operating capability not later than October 1, 2013.

''(d) REPORT.—Not later than 90 days after the date of the enactment of this Act [Dec. 31, 2011], 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 that includes—

''(1) the implementation plan for the program established under subsection (a);

''(2) the resources required to implement the program;

''(3) specific efforts to ensure that implementation does not negatively impact activities in support of ongoing operations in areas of hostilities;

''(4) a definition of the capabilities that will be achieved at initial operating capability and full operating capability, respectively; and

''(5) a description of any other issues related to such implementation that the Secretary considers appropriate.

''(e) BRIEFING REQUIREMENT.—The Secretary shall provide briefings to the Committees on Armed Services of the House of Representatives and the Senate as follows:

''(1) Not later than 90 days after the date of the enactment of this Act [Dec. 31, 2011], a briefing describing the governance structure referred to in subsection (b)(3).

''(2) Not later than 120 days after the date of the enactment of this Act, a briefing detailing the inventory and status of technology solutions deployment referred to in subsection (b)(1), including an identification of the total number of host platforms planned for such deployment, the current number of host platforms that provide appropriate security, and the funding and timeline for remaining deployment.

''(3) Not later than 180 days after the date of the enactment of this Act, a briefing detailing the policies and procedures referred to in subsection (b)(2), including an assessment of the effectiveness of such policies and procedures and an assessment of the potential impact of such policies and procedures on information sharing within the Department of Defense and with interagency and international partners.

''(f) BUDGET SUBMISSION.—On the date on which the President submits to Congress the budget under section 1105 of title 31, United States Code, for each of fiscal years 2014 through 2019, 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] an identification of the resources requested in such budget to carry out the program established under subsection (a).''

STRATEGY TO ACQUIRE CAPABILITIES TO DETECT PREVIOUSLY UNKNOWN CYBER ATTACKS

Pub. L. 112–81, div. A, title IX, §953, Dec. 31, 2011, 125 Stat. 1550, provided that:

''(a) IN GENERAL.—The Secretary of Defense shall develop and implement a plan to augment the cybersecurity strategy of the Department of Defense through the acquisition of advanced capabilities to discover and isolate penetrations and attacks that were previously unknown and for which signatures have not been developed for incorporation into computer intrusion detection and prevention systems and anti-virus software systems.

''(b) CAPABILITIES.—

''(1) NATURE OF CAPABILITIES.—The capabilities to be acquired under the plan required by subsection (a) shall—

''(A) be adequate to enable well-trained analysts to discover the sophisticated attacks conducted by nation-state adversaries that are categorized as 'advanced persistent threats';

''(B) be appropriate for—

''(i) endpoints or hosts;

''(ii) network-level gateways operated by the Defense Information Systems Agency where the Department of Defense network connects to the public Internet; and

''(iii) global networks owned and operated by private sector Tier 1 Internet Service Providers;

''(C) at the endpoints or hosts, add new discovery capabilities to the Host-Based Security System of the Department, including capabilities such as—

''(i) automatic blocking of unauthorized software programs and accepting approved and vetted programs;

''(ii) constant monitoring of all key computer attributes, settings, and operations (such as registry keys, operations running in memory, security settings, memory tables, event logs, and files); and

''(iii) automatic baselining and remediation of altered computer settings and files;

''(D) at the network-level gateways and internal network peering points, include the sustainment and enhancement of a system that is based on full-packet capture, session reconstruction, extended storage, and advanced analytic tools, by—

''(i) increasing the number and skill level of the analysts assigned to query stored data, whether by contracting for security services, hiring and training Government personnel, or both; and

''(ii) increasing the capacity of the system to handle the rates for data flow through the gateways and the storage requirements specified by the United States Cyber Command; and

''(E) include the behavior-based threat detection capabilities of Tier 1 Internet Service Providers and other companies that operate on the global Internet.

''(2) SOURCE OF CAPABILITIES.—The capabilities to be acquired shall, to the maximum extent practicable, be acquired from commercial sources. In making decisions on the procurement of such capabilities from among competing commercial and Government providers, the Secretary shall take into consideration the needs of other departments and agencies of the Federal Government, State and local governments, and critical infrastructure owned and operated by the private sector for unclassified, affordable, and sustainable commercial solutions.

''(c) INTEGRATION AND MANAGEMENT OF DISCOVERY CAPABILITIES.—The plan required by subsection (a) shall include mechanisms for improving the standardization, organization, and management of the security information and event management systems that are widely deployed across the Department of Defense to improve the ability of United States Cyber Command to understand and control the status and condition of Department networks, including mechanisms to ensure that the security information and event management systems of the Department receive and correlate data collected and analyses conducted at the host or endpoint, at the network gateways, and by Internet Service Providers in order to discover new attacks reliably and rapidly.

''(d) PROVISION FOR CAPABILITY DEMONSTRATIONS.—The plan required by subsection (a) shall provide for the conduct of demonstrations, pilot projects, and other tests on cyber test ranges and operational networks in order to determine and verify that the capabilities to be acquired pursuant to the plan are effective, practical, and affordable.

''(e) REPORT.—Not later than April 1, 2012, the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the plan required by subsection (a). The report shall set forth the plan and include a comprehensive description of the actions being undertaken by the Department to implement the plan.''

STRATEGY ON COMPUTER SOFTWARE ASSURANCE

Pub. L. 111–383, div. A, title IX, § 932, Jan. 7, 2011, 124 Stat. 4335, provided that:

''(a) STRATEGY REQUIRED.—The Secretary of Defense shall develop and implement, by not later than October 1, 2011, a strategy for assuring the security of software and software-based applications for all covered systems.

''(b) COVERED SYSTEMS.—For purposes of this section, a covered system is any critical information system or weapon system of the Department of Defense, including the following:

''(1) A major system, as that term is defined in section 2302(5) of title 10, United States Code.

''(2) A national security system, as that term is defined in section 3542(b)(2) of title 44, United States Code.

''(3) Any Department of Defense information system categorized as Mission Assurance Category I.

''(4) Any Department of Defense information system categorized as Mission Assurance Category II in accordance with Department of Defense Directive 8500.01E.

''(c) ELEMENTS.—The strategy required by subsection (a) shall include the following:

''(1) Policy and regulations on the following:

''(A) Software assurance generally.

''(B) Contract requirements for software assurance for covered systems in development and production.

''(C) Inclusion of software assurance in milestone reviews and milestone approvals.

''(D) Rigorous test and evaluation of software assurance in development, acceptance, and operational tests.

''(E) Certification and accreditation requirements for software assurance for new systems and for updates for legacy systems, including mechanisms to monitor and enforce reciprocity of certification and accreditation processes among the military departments and Defense Agencies.

''(F) Remediation in legacy systems of critical software assurance deficiencies that are defined as critical in accordance with the Application Security Technical Implementation Guide of the Defense Information Systems Agency.

''(2) Allocation of adequate facilities and other resources for test and evaluation and certification and accreditation of software to meet applicable requirements for research and development, systems acquisition, and operations.

''(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 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 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.

[1] See References in Text note below.

§ 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—

(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—