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

''(d) REPORT TO CONGRESS.—Not later than one year after the date of the enactment of this Act [Jan. 28, 2008], the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the implementation of this section.''

§ 2224. Defense Information Assurance Program

(a) DEFENSE INFORMATION ASSURANCE PROGRAM.—The Secretary of Defense shall carry out a program, to be known as the ''Defense Information Assurance Program'', to protect and defend Department of Defense information, information systems, and information networks that are critical to the Department and the armed forces during day-to-day operations and operations in times of crisis.

(b) OBJECTIVES OF THE PROGRAM.—The objectives of the program shall be to provide continuously for the availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Infrastructure.

(c) PROGRAM STRATEGY.—In carrying out the program, the Secretary shall develop a program strategy that encompasses those actions necessary to assure the readiness, reliability, continuity, and integrity of Defense information systems, networks, and infrastructure, including through compliance with subchapter II of chapter 35 of title 44, including through compliance with subchapter III of chapter 35 of title 44. The program strategy shall include the following:

(1) A vulnerability and threat assessment of elements of the defense and supporting nondefense information infrastructures that are essential to the operations of the Department and the armed forces.

(2) Development of essential information assurances technologies and programs.

(3) Organization of the Department, the armed forces, and supporting activities to defend against information warfare.

(4) Joint activities of the Department with other departments and agencies of the Government, State and local agencies, and elements of the national information infrastructure.

(5) The conduct of exercises, war games, simulations, experiments, and other activities designed to prepare the Department to respond to information warfare threats.

(6) Development of proposed legislation that the Secretary considers necessary for implementing the program or for otherwise responding to the information warfare threat.

(d) COORDINATION.—In carrying out the program, the Secretary shall coordinate, as appropriate, with the head of any relevant Federal agency and with representatives of those national critical information infrastructure systems that are essential to the operations of the Department and the armed forces on information assurance measures necessary to the protection of these systems.

[(e) Repealed. Pub. L. 108–136, div. A, title X, §1031(a)(12), Nov. 24, 2003, 117 Stat. 1597.]

(f) INFORMATION ASSURANCE TEST BED.—The Secretary shall develop an information assurance test bed within the Department of Defense to provide—

(1) an integrated organization structure to plan and facilitate the conduct of simulations, war games, exercises, experiments, and other activities to prepare and inform the Department regarding information warfare threats; and

(2) organization and planning means for the conduct by the Department of the integrated or joint exercises and experiments with elements of the national information systems infrastructure and other non-Department of Defense organizations that are responsible for the oversight and management of critical information systems and infrastructures on which the Department, the armed forces, and supporting activities depend for the conduct of daily operations and operations during crisis.

(Added Pub. L. 106–65, div. A, title X, §1043(a), Oct. 5, 1999, 113 Stat. 760; amended Pub. L. 106–398, §1 [[div. A], title X, §1063], Oct. 30, 2000, 114 Stat. 1654, 1654A–274; Pub. L. 107–296, title X, §1001(c)(1)(B), Nov. 25, 2002, 116 Stat. 2267; Pub. L. 107–347, title III, §301(c)(1)(B), Dec. 17, 2002, 116 Stat. 2955; Pub. L. 108–136, div. A, title X, §1031(a)(12), Nov. 24, 2003, 117 Stat. 1597; Pub. L. 108–375, div. A, title X, §1084(d)(17), Oct. 28, 2004, 118 Stat. 2062.)

AMENDMENTS

2004—Subsec. (c). Pub. L. 108–375 substituted ''subchapter II'' for ''subtitle II'' in introductory provisions.

2003—Subsec. (e). Pub. L. 108–136 struck out subsec. (e) which directed the Secretary of Defense to annually submit to Congress a report on the Defense Information Assurance Program.

2002—Subsec. (b). Pub. L. 107–296, §1001(c)(1)(B)(i), and Pub. L. 107–347, §301(c)(1)(B)(i), amended subsec. (b) identically, substituting ''Objectives of the Program'' for ''Objectives and Minimum Requirements'' in heading and striking out par. (1) designation before ''The objectives''.

Subsec. (b)(2). Pub. L. 107–347, §301(c)(1)(B)(ii), struck out par. (2) which read as follows: ''The program shall at a minimum meet the requirements of sections 3534 and 3535 of title 44.''

Pub. L. 107–296, §1001(c)(1)(B)(ii), which directed the striking out of ''(2) the program shall at a minimum meet the requirements of section 3534 and 3535 of title 44, United States Code.'' could not be executed. See above par.

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

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

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

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

EFFECTIVE DATE OF 2002 AMENDMENT

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

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, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of Title 44, Public Printing and Documents.

PROCEDURES AND REPORTING REQUIREMENT ON CYBERSECURITY BREACHES AND LOSS OF PERSONALLY IDENTIFIABLE INFORMATION AND CONTROLLED UNCLASSIFIED INFORMATION

Pub. L. 115–232, div. A, title XVI, §1639, Aug. 13, 2018, 132 Stat. 2129, provided that:

''(a) IN GENERAL.—In the event of a significant loss of personally identifiable information of civilian or uniformed members of the Armed Forces, or a significant loss of controlled unclassified information by a cleared defense contractor, the Secretary of Defense shall promptly submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] notice in writing of such loss. Such notice may be submitted in classified or unclassified formats.

''(b) PROCEDURES.—Not later than 180 days after the date of the enactment of this Act [Aug. 13, 2018], the Secretary of Defense shall establish and submit to the congressional defense committees procedures for complying with the requirement of subsection (a). Such procedures shall be consistent with the national security of the United States, the protection of operational integrity, the protection of personally identifiable information of civilian and uniformed members of the Armed Forces, and the protection of controlled unclassified information.

''(c) DEFINITIONS.—In this section:

''(1) SIGNIFICANT LOSS OF CONTROLLED UNCLASSIFIED INFORMATION.—The term 'significant loss of controlled unclassified information' means an intentional, accidental, or otherwise known theft, loss, or disclosure of Department of Defense programmatic or technical controlled unclassified information the loss of which would have significant impact or consequence to a program or mission of the Department of Defense, or the loss of which is of substantial volume.

''(2) SIGNIFICANT LOSS OF PERSONALLY IDENTIFIABLE INFORMATION.—The term 'significant loss of personally identifiable information' means an intentional, accidental, or otherwise known disclosure of information that can be used to distinguish or trace an individual's identity, such as the name, Social Security number, date and place of birth, biometric records, home or other phone numbers, or other demographic, personnel, medical, or financial information, involving 250 or more civilian or uniformed members of the Armed Forces.''

MATTERS PERTAINING TO THE SHARKSEER CYBERSECURITY PROGRAM

Pub. L. 115–232, div. A, title XVI, §1641, Aug. 13, 2018, 132 Stat. 2131, provided that:

''(a) TRANSFER OF PROGRAM.—Not later than March 1, 2019, the Secretary of Defense shall transfer the operations and maintenance for the Sharkseer cybersecurity program from the National Security Agency to the Defense Information Systems Agency, including all associated funding and, as the Secretary considers necessary, personnel.

''(b) LIMITATION ON FUNDING FOR THE INFORMATION SYSTEMS SECURITY PROGRAM.—Of the funds authorized to be appropriated by this Act [see Tables for classification] or otherwise made available for fiscal year 2019 or any subsequent fiscal year for research, development, test, and evaluation for the Information Systems Security Program for the National Security Agency, not more than 90 percent may be obligated or expended unless the Chief of Information Officer, in consultation with the Principal Cyber Advisor, certifies to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] that the operations and maintenance funding for the Sharkseer program for fiscal year 2019 and the subsequent fiscal years of the current Future Years Defense Program are available or programmed.

''(c) REPORT.—Not later than 90 days after the date of the enactment of this Act [Aug. 13, 2018], the Chief Information Officer shall provide to the congressional defense committees a report that assesses the transition of base operations of the SharkSeer program to the Defense Information Systems Agency, including with respect to staffing, acquisition, contracts, sensor management, and the ability to conduct cyber threat analyses and detect advanced malware. Such report shall also include a plan for continued capability development.

''(d) SHARKSEER BREAK AND INSPECT CAPABILITY.—

''(1) IN GENERAL.—The Secretary of Defense shall ensure that the decryption capability described in section 1636 of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113–291) [128 Stat. 3644] is provided by the break and inspect subsystem of the Sharkseer cybersecurity program, unless the Chief of Information Officer, in consultation with the Principal Cyber Advisor, notifies the congressional defense committees on or before the date that is 90 days after the date of the enactment of this Act that a superior enterprise solution will be operational before October 1, 2019.

''(2) INTEGRATION OF CAPABILITY.—The Secretary shall take such actions as are necessary to integrate the break and inspect subsystem of the Sharkseer cybersecurity program with the Department of Defense public key infrastructure.

''(e) VISIBILITY TO ENDPOINTS.—The Secretary shall take such actions as are necessary to enable, by October 1, 2020, the Sharkseer cybersecurity program and computer network defense service providers to instantly and automatically determine the specific identity and location of computer hosts and other endpoints that received or sent malware detected by the Sharkseer cybersecurity program or other network perimeter defenses.

''(f) SANDBOX AS A SERVICE.—The Secretary shall use the Sharkseer cybersecurity program sandbox-as-a-service capability as an enterprise solution and terminate all other such projects, unless the Chief of Information Officer, in consultation with the Principal Cyber Advisor, notifies the congressional defense committees on or before the date that is 90 days after the date of the enactment of this Act that a superior enterprise solution will be operational before October 1, 2019.''

DESIGNATION OF OFFICIAL FOR MATTERS RELATING TO INTEGRATING CYBERSECURITY AND INDUSTRIAL CONTROL SYSTEMS WITHIN THE DEPARTMENT OF DEFENSE

Pub. L. 115–232, div. A, title XVI, §1643, Aug. 13, 2018, 132 Stat. 2133, provided that:

''(a) DESIGNATION OF INTEGRATING OFFICIAL.—Not later than 180 days after the date of the enactment of this Act [Aug. 13, 2018], the Secretary of Defense shall designate one official to be responsible for matters relating to integrating cybersecurity and industrial control systems for the Department of Defense.

''(b) RESPONSIBILITIES.—The official designated pursuant to subsection (a) shall be responsible for matters described in such subsection at all levels of command, from the Department's leadership to the facilities owned by or operated on behalf of the Department of Defense using industrial control systems, including developing Department-wide certification standards for integration of industrial control systems and taking into consideration frameworks set forth by the Na-

tional Institute of Standards and Technology for the cybersecurity of such systems.''

ASSISTANCE FOR SMALL MANUFACTURERS IN THE DEFENSE INDUSTRIAL SUPPLY CHAIN AND UNIVERSITIES ON MATTERS RELATING TO CYBERSECURITY

Pub. L. 115–232, div. A, title XVI, §1644, Aug. 13, 2018, 132 Stat. 2133, provided that:

''(a) DISSEMINATION OF CYBERSECURITY RESOURCES.—

''(1) IN GENERAL.—The Secretary of Defense, in consultation with the Director of the National Institute of Standards and Technology, shall take such actions as may be necessary to enhance awareness of cybersecurity threats among small manufacturers and universities working on Department of Defense programs and activities.

''(2) PRIORITY.—The Secretary of Defense shall prioritize efforts to increase awareness to help reduce cybersecurity risks faced by small manufacturers and universities referred to in paragraph (1).

''(3) SECTOR FOCUS.—The Secretary of Defense shall carry out this subsection with a focus on such small manufacturers and universities as the Secretary considers critical.

''(4) OUTREACH EVENTS.—Under paragraph (1), the Secretary of Defense shall conduct outreach to support activities consistent with this section. Such outreach may include live events with a physical presence and outreach conducted through Internet websites. Such outreach may include training, including via courses and classes, to help small manufacturers and universities improve their cybersecurity.

''(5) ROADMAPS AND ASSESSMENTS.—The Secretary of Defense shall ensure that cybersecurity for defense industrial base manufacturing is included in appropriate research and development roadmaps and threat assessments.

''(b) VOLUNTARY CYBERSECURITY SELF-ASSESSMENTS.—The Secretary of Defense shall develop mechanisms to provide assistance to help small manufacturers and universities conduct voluntary self-assessments in order to understand operating environments, cybersecurity requirements, and existing vulnerabilities, including through the Mentor Protégé Program, small business programs, and engagements with defense laboratories and test ranges.

''(c) TRANSFER OF RESEARCH FINDINGS AND EXPERTISE.—

''(1) IN GENERAL.—The Secretary of Defense shall promote the transfer of appropriate technology, threat information, and cybersecurity techniques developed in the Department of Defense to small manufacturers and universities throughout the United States to implement security measures that are adequate to protect covered defense information, including controlled unclassified information.

''(2) COORDINATION WITH OTHER FEDERAL EXPERTISE AND CAPABILITIES.—The Secretary of Defense shall coordinate efforts, when appropriate, with the expertise and capabilities that exist in Federal agencies and federally sponsored laboratories.

''(3) AGREEMENTS.—In carrying out this subsection, the Secretary of Defense may enter into agreements with private industry, institutes of higher education, or a State, United States territory, local, or tribal government to ensure breadth and depth of coverage to the United States defense industrial base and to leverage resources.

''(d) DEFENSE ACQUISITION WORKFORCE CYBER TRAINING PROGRAM.—The Secretary of Defense shall establish a cyber counseling certification program, or approve a similar existing program, to certify small business professionals and other relevant acquisition staff within the Department of Defense to provide cyber planning assistance to small manufacturers and universities.

''(e) ESTABLISHMENT OF CYBERSECURITY FOR DEFENSE INDUSTRIAL BASE MANUFACTURING ACTIVITY.—

''(1) AUTHORITY.—The Secretary of Defense may establish an activity to assess and strengthen the cybersecurity resiliency of the defense industrial base, if the Secretary determines such is appropriate.

''(2) DESIGNATION.—The activity described in paragraph (1), if established, shall be known as the 'Cybersecurity for Defense Industrial Base Manufacturing Activity'.

''(3) SPECIFICATION.—The Cybersecurity for Defense Industrial Base Manufacturing Activity, if established, shall implement the requirements specified in subsections (a) through (c).

''(f) AUTHORITIES.—In carrying out this section, the Secretary may use the following authorities:

''(1) The Manufacturing Technology Program established under section 2521 of title 10, United States Code.

''(2) The Centers for Science, Technology, and Engineering Partnership program under section 2368 of title 10, United States Code.

''(3) The Manufacturing Engineering Education Program established under section 2196 of title 10, United States Code.

''(4) The Small Business Innovation Research program.

''(5) The mentor-protégé program.

''(6) Other legal authorities as the Secretary determines necessary to effectively and efficiently carry out this section.

''(g) DEFINITIONS.—In this section:

''(1) RESOURCES.—The term 'resources' means guidelines, tools, best practices, standards, methodologies, and other ways of providing information.

''(2) SMALL BUSINESS CONCERN.—The term 'small business concern' means a small business concern as that term is used in section 3 of the Small Business Act (15 U.S.C. 632).

''(3) SMALL MANUFACTURER.—The term 'small manufacturer' means a small business concern that is a manufacturer in the defense industrial supply chain.

''(4) STATE.—The term 'State' means each of the several States, Territories, and possessions of the United States, the District of Columbia, and the Commonwealth of Puerto Rico.''

EMAIL AND INTERNET WEBSITE SECURITY AND AUTHENTICATION

Pub. L. 115–232, div. A, title XVI, §1645, Aug. 13, 2018, 132 Stat. 2135, provided that:

''(a) IMPLEMENTATION OF PLAN REQUIRED.—Except as provided by subsection (b), the Secretary of Defense shall develop and implement the plan outlined in Binding Operational Directive 18–01, issued by the Secretary of Homeland Security on October 16, 2017, relating to email security and authentication and Internet website security, according to the schedule established by the Binding Operational Directive for the rest of the Executive Branch beginning with the date of enactment of this Act [Aug. 13, 2018].

''(b) WAIVER.—The Secretary may waive the requirements of subsection (a) if the Secretary submits to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives], the Committee on Oversight and Government Reform of the House of Representatives, and the Committee on Homeland Security and Government Affairs of the Senate a certification that existing or planned security measures for the Department of Defense either meet or exceed the information security requirements of Binding Operational Directive 18–01.

''(c) FUTURE BINDING OPERATIONAL DIRECTIVES.—The Chief Information Officer of the Department of Defense shall notify the congressional defense committees, the Committee on Oversight and Government Reform of the House of Representatives, and the Committee on Homeland Security and Government Affairs of the Senate within 180 days of the issuance by the Secretary of Homeland Security after the date of the enactment of this Act of any Binding Operational Directive for cybersecurity whether the Department of Defense will comply with the Directive or how the Department of

Defense plans to meet or exceed the security objectives of the Directive.''

RISK THRESHOLDS FOR SYSTEMS AND NETWORK OPERATIONS

Pub. L. 115–232, div. A, title XVI, §1647(c), Aug. 13, 2018, 132 Stat. 2136, provided that: ''The Chief Information Officer of the Department of Defense, in coordination with the Principal Cyber Advisor, the Director of Operations of the Joint Staff, and the Commander of United States Cyber Command, shall establish risk thresholds for systems and network operations that, when exceeded, would trigger heightened security measures, such as enhanced monitoring and access policy changes.''

MITIGATION OF RISKS TO NATIONAL SECURITY POSED BY PROVIDERS OF INFORMATION TECHNOLOGY PRODUCTS AND SERVICES WHO HAVE OBLIGATIONS TO FOREIGN GOVERNMENTS

Pub. L. 115–232, div. A, title XVI, §1655, Aug. 13, 2018, 132 Stat. 2149, provided that:

''(a) DISCLOSURE REQUIRED.—Subject to the regulations issued under subsection (b), the Department of Defense may not use a product, service, or system procured or acquired after the date of the enactment of this Act [Aug. 13, 2018] relating to information or operational technology, cybersecurity, an industrial control system, or weapons system provided by a person unless that person discloses to the Secretary of Defense the following:

''(1) Whether, and if so, when, within five years before or at any time after the date of the enactment of this Act, the person has allowed a foreign government to review the code of a non-commercial product, system, or service developed for the Department, or whether the person is under any obligation to allow a foreign person or government to review the code of a non-commercial product, system, or service developed for the Department as a condition of entering into an agreement for sale or other transaction with a foreign government or with a foreign person on behalf of such a government.

''(2) Whether, and if so, when, within five years before or at any time after the date of the enactment of this Act, the person has allowed a foreign government listed in section 1654 [of Pub. L. 115–232, 10 U.S.C. 394 note] to review the source code of a product, system, or service that the Department is using or intends to use, or is under any obligation to allow a foreign person or government to review the source code of a product, system, or service that the Department is using or intends to use as a condition of entering into an agreement for sale or other transaction with a foreign government or with a foreign person on behalf of such a government.

''(3) Whether or not the person holds or has sought a license pursuant to the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations, or successor regulations, for information technology products, components, software, or services that contain code custom-developed for the non-commercial product, system, or service the Department is using or intends to use.

''(b) REGULATIONS.—

''(1) IN GENERAL.—The Secretary of Defense shall issue regulations regarding the implementation of subsection (a).

''(2) UNIFORM REVIEW PROCESS.—If information obtained from a person under subsection (a) or the contents of the registry under subsection (f) are the subject of a request under section 552 of title 5, United States Code (commonly referred to as the 'Freedom of Information Act'), the Secretary of Defense shall conduct a uniform review process, without regard to the office holding the information, to determine if the information is exempt from disclosure under such section 552.

''(c) PROCUREMENT.—Procurement contracts for covered products or systems shall include a clause requiring the information contained in subsection (a) be disclosed during the period of the contract if an entity becomes aware of information requiring disclosure required pursuant to such subsection, including any mitigation measures taken or anticipated.

''(d) MITIGATION OF RISKS.—

''(1) IN GENERAL.—If, after reviewing a disclosure made by a person under subsection (a), the Secretary determines that the disclosure relating to a product, system, or service entails a risk to the national security infrastructure or data of the United States, or any national security system under the control of the Department, the Secretary shall take such measures as the Secretary considers appropriate to mitigate such risks, including, as the Secretary considers appropriate, by conditioning any agreement for the use, procurement, or acquisition of the product, system, or service on the inclusion of enforceable conditions or requirements that would mitigate such risks.

''(2) THIRD-PARTY TESTING STANDARD.—Not later than two years after the date of the enactment of this Act the Secretary shall develop such third-party testing standard as the Secretary considers acceptable for commercial off the shelf (COTS) products, systems, or services to use when dealing with foreign governments.

''(e) EXEMPTION OF OPEN SOURCE SOFTWARE.—This section shall not apply to open source software.

''(f) ESTABLISHMENT OF REGISTRY.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall—

''(1) establish within the operational capabilities of the Committee for National Security Systems (CNSS) or within such other agency as the Secretary considers appropriate a registry containing the information disclosed under subsection (a); and

''(2) upon request, make such information available to any agency conducting a procurement pursuant to the Federal Acquisition Regulations or the Defense Federal Acquisition Regulations.

''(g) ANNUAL REPORTS.—Not later than one year after the date of the enactment of this Act and not less frequently than once each year thereafter, the Secretary of Defense shall submit to the appropriate committees of Congress a report detailing the number, scope, product classifications, and mitigation agreements related to each product, system, and service for which a disclosure is made under subsection (a).

''(h) DEFINITIONS.—In this section:

''(1) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—The term 'appropriate committees of Congress' means—

''(A) the Committee on Armed Services, the Select Committee on Intelligence, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

''(B) the Committee on Armed Services, the Permanent Select Committee on Intelligence, the Committee on Homeland Security, and the Committee on Oversight and Government Reform of the House of Representatives.

''(2) COMMERCIAL ITEM.—The term 'commercial item' has the meaning given such term in section 103 of title 41, United States Code.

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

''(4) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given such term in section 3552(b) of title 44, United States Code.

''(5) NON-COMMERCIAL PRODUCT, SYSTEM, OR SERVICE.—The term 'non-commercial product, system, or service' means a product, system, or service that does not meet the criteria of a commercial item.

''(6) OPEN SOURCE SOFTWARE.—The term 'open source software' means software for which the

human-readable source code is available for use, study, re-use, modification, enhancement, and re-distribution by the users of such software.''

INTEGRATION OF STRATEGIC INFORMATION OPERATIONS AND CYBER-ENABLED INFORMATION OPERATIONS

Pub. L. 115–91, div. A, title XVI, §1637, Dec. 12, 2017, 131 Stat. 1742, provided that:

''(a) PROCESSES AND PROCEDURES FOR INTEGRATION.—

''(1) IN GENERAL.—The Secretary of Defense shall—

''(A) establish processes and procedures to integrate strategic information operations and cyber-enabled information operations across the elements of the Department of Defense responsible for such operations, including the elements of the Department responsible for military deception, public affairs, electronic warfare, and cyber operations; and

''(B) ensure that such processes and procedures provide for integrated Defense-wide strategy, planning, and budgeting with respect to the conduct of such operations by the Department, including activities conducted to counter and deter such operations by malign actors.

''(2) DESIGNATED SENIOR OFFICIAL.—The Secretary of Defense shall designate a senior official of the Department of Defense (in this section referred to as the 'designated senior official') who shall implement and oversee the processes and procedures established under paragraph (1). The designated senior official shall be selected by the Secretary from among individuals serving in the Department of Defense at or below the level of an Under Secretary of Defense.

''(3) RESPONSIBILITIES.—The designated senior official shall have, with respect to the implementation and oversight of the processes and procedures established under paragraph (1), the following responsibilities:

''(A) Oversight of strategic policy and guidance.

''(B) Overall resource management for the integration of information operations and cyber-enabled information operations of the Department.

''(C) Coordination with the head of the Global Engagement Center to support the purpose of the Center (as described [in] section 1287(a)(2) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 22 U.S.C. 2656 note)) and liaison with the Center and other relevant Federal Government entities to support such purpose.

''(D) Development of a strategic framework for the conduct of information operations by the Department of Defense, including cyber-enabled information operations, coordinated across all relevant elements of the Department of Defense, including both near-term and long-term guidance for the conduct of such coordinated operations.

''(E) Development and dissemination of a common operating paradigm across the elements of the Department of Defense specified in paragraph (1) to counter the influence, deception, and propaganda activities of key malign actors, including in cyberspace.

''(F) Development of guidance for, and promotion of, the capability of the Department of Defense to liaison with the private sector, including social media, on matters relating to the influence activities of malign actors.

''(b) REQUIREMENTS AND PLANS FOR INFORMATION OPERATIONS.—

''(1) COMBATANT COMMAND PLANNING AND REGIONAL STRATEGY.—(A) The Secretary shall require each commander of a combatant command to develop, in coordination with the relevant regional Assistant Secretary of State or Assistant Secretaries of State and with the assistance of the Coordinator of the Global Engagement Center and the designated senior official, a regional information strategy and interagency coordination plan for carrying out the strategy, where applicable.

''(B) The Secretary shall require each commander of a combatant command to develop such requirements and specific plans as may be necessary for the conduct of information operations in support of the strategy required under subparagraph (A), including plans for deterring information operations, including deterrence in the cyber domain, by malign actors against the United States, allies of the United States, and interests of the United States.

''(2) IMPLEMENTATION PLAN FOR DOD STRATEGY FOR OPERATIONS IN THE INFORMATION ENVIRONMENT.—

''(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 12, 2017], the designated senior official shall—

''(i) review the strategy of the Department of Defense titled 'Department of Defense Strategy for Operations in the Information Environment' and dated June 2016; and

''(ii) submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a plan for implementation of such strategy.

''(B) ELEMENTS.—The plan required under subparagraph (A) shall include, at a minimum, the following:

''(i) An accounting of the efforts undertaken in support of the strategy described in subparagraph (A)(i) in the period since it was issued in June 2016.

''(ii) A description of any updates or changes to such strategy that have been made since it was first issued, as well as any expected updates or changes resulting from the designation of the designated senior official.

''(iii) A description of the role of the Department of Defense as part of a broader whole-of-Government strategy for strategic communications, including a description of any assumptions about the roles and contributions of other departments and agencies of the Federal Government with respect to such a strategy.

''(iv) Defined actions, performance metrics, and projected timelines for achieving each of the 15 tasks specified in the strategy described in subparagraph (A)(i).

''(v) An analysis of any personnel, resourcing, capability, authority, or other gaps that will need to be addressed to ensure effective implementation of the strategy described in subparagraph (A)(i) across all relevant elements of the Department of Defense.

''(vi) An investment framework and projected timeline for addressing any gaps identified under clause (v).

''(vii) Such other matters as the Secretary of Defense considers relevant.

''(C) PERIODIC STATUS REPORTS.—Not less frequently than once every 90 days during the three-year period beginning on the date on which the implementation plan is submitted under subparagraph (A)(ii), the designated senior official shall submit to the congressional defense committees a report describing the status of the efforts of the Department of Defense in accomplishing the tasks specified under clauses (iv) and (vi) of subparagraph (B).

''(c) TRAINING AND EDUCATION.—Consistent with the elements of the implementation plan under paragraph (2), the designated senior official shall recommend the establishment of programs to provide training and education to such members of the Armed Forces and civilian employees of the Department of Defense as the Secretary considers appropriate to ensure that such members and employees understand the role of information in warfare, the central goal of all military operations to affect the perceptions, views, and decision making of adversaries, and the effective management and conduct of operations in the information environment.''

EXERCISE ON ASSESSING CYBERSECURITY SUPPORT TO ELECTION SYSTEMS OF STATES

Pub. L. 115–91, div. A, title XVI, §1638, Dec. 12, 2017, 131 Stat. 1744, provided that:

''(a) INCLUSION OF CYBER VULNERABILITIES IN ELECTION SYSTEMS IN CYBER GUARD EXERCISES.—Subject to subsection (b), the Secretary of Defense, in consultation with the Secretary of Homeland Security, may carry out exercises relating to the cybersecurity of election systems of States as part of the exercise commonly known as the 'Cyber Guard Exercise'.

''(b) AGREEMENT REQUIRED.—The Secretary of Defense may carry out an exercise relating to the cybersecurity of a State's election system under subsection (a) only if the State enters into a written agreement with the Secretary under which the State—

''(1) agrees to participate in such exercise; and

''(2) agrees to allow vulnerability testing of the components of the State's election system.

''(c) REPORT.—Not later than 90 days after the completion of any Cyber Guard Exercise, 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 ability of the National Guard to assist States, if called upon, in defending election systems from cyberattacks. Such report shall include a description of the capabilities, readiness levels, and best practices of the National Guard with respect to the prevention of cyber attacks on State election systems.''

MEASUREMENT OF COMPLIANCE WITH CYBERSECURITY REQUIREMENTS FOR INDUSTRIAL CONTROL SYSTEMS

Pub. L. 115–91, div. A, title XVI, §1639, Dec. 12, 2017, 131 Stat. 1744, provided that:

''(a) IN GENERAL.—Not later than January 1, 2018, the Secretary of Defense shall make such changes to the cybersecurity scorecard as are necessary to ensure that the Secretary measures the progress of each element of the Department of Defense in securing the industrial control systems of the Department against cyber threats, including such industrial control systems as supervisory control and data acquisition systems, distributed control systems, programmable logic controllers, and platform information technology.

''(b) CYBERSECURITY SCORECARD DEFINED.—In this section, the term 'cybersecurity scorecard' means the Department of Defense Cybersecurity Scorecard used by the Department to measure compliance with cybersecurity requirements as described in the plan of the Department titled 'Department of Defense Cybersecurity Discipline Implementation Plan'.''

STRATEGIC CYBERSECURITY PROGRAM

Pub. L. 115–91, div. A, title XVI, §1640, Dec. 12, 2017, 131 Stat. 1745, provided that:

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 12, 2017], the Secretary of Defense, in consultation with the Director of the National Security Agency, shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a plan for the establishment of a program to be known as the 'Strategic Cybersecurity Program' or 'SCP' (in this section referred to as the 'Program').

''(b) ELEMENTS.—The Program shall be comprised of personnel assigned to the Program by the Secretary of Defense from among personnel, including regular and reserve members of the Armed Forces, civilian employees of the Department, and personnel of the research laboratories of the Department of Defense and the Department of Energy, who have particular expertise in the areas of responsibility described in subsection (c). Any personnel assigned to the Program from among personnel of the Department of Energy shall be so assigned with the concurrence of the Secretary of Energy.

''(c) RESPONSIBILITIES.—

''(1) IN GENERAL.—Personnel assigned to the Program shall assist the Department of Defense in improving the cybersecurity of the following systems of the Federal Government:

''(A) Offensive cyber systems.

''(B) Long-range strike systems.

''(C) Nuclear deterrent systems.

''(D) National security systems.

''(E) Critical infrastructure of the Department of Defense (as that term is defined in section 1650(f)(1) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 10 U.S.C. 2224 note)).

''(2) REVIEWS OF SYSTEMS AND INFRASTRUCTURE.—In carrying out the activities described in paragraph (1), the personnel assigned to the Program shall conduct appropriate reviews of existing systems and infrastructure and acquisition plans for proposed systems and infrastructure. The review of an acquisition plan for any proposed system or infrastructure shall be carried out before Milestone B approval for such system or infrastructure.

''(3) RESULTS OF REVIEWS.—The results of each review carried out under paragraph (2), including any remedial action recommended pursuant to such review, shall be made available to any agencies or organizations of the Department involved in the development, procurement, operation, or maintenance of the system or infrastructure concerned.

''(d) INTEGRATION WITH OTHER EFFORTS.—The plan required under subsection (a) shall build upon, and shall not duplicate, other efforts of the Department of Defense relating to cybersecurity, including—

''(1) the evaluation of cyber vulnerabilities of major weapon systems of the Department of Defense required under section 1647 of the National Defense Authorization Act for Fiscal Year 2016 ([Public Law] 114–92; 129 Stat. 1118 [set out as a note below]);

''(2) the evaluation of cyber vulnerabilities of Department of Defense critical infrastructure required under section 1650 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 10 U.S.C. 2224 note); and

''(3) the activities of the cyber protection teams of the Department of Defense.

''(e) REPORT.—Not later than one year after the date on which the plan is submitted to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] under subsection (a), the Secretary of Defense shall submit to the congressional defense committees a report on any activities carried out pursuant to such plan. The report shall include the following:

''(1) A description of any activities of the Program carried out pursuant to the plan during the time period covered by the report.

''(2) A description of particular challenges encountered in the course of the activities of the Program, if any, and of actions taken to address such challenges.

''(3) A description of any plans for additional activities under the Program.''

REQUIREMENT TO ENTER INTO AGREEMENTS RELATING TO USE OF CYBER OPPOSITION FORCES

Pub. L. 114–328, div. A, title XVI, §1644, Dec. 23, 2016, 130 Stat. 2602, provided that:

''(a) REQUIREMENT FOR AGREEMENTS.—Not later than September 30, 2017, the Secretary of Defense shall ensure that each commander of a combatant command establishes appropriate agreements with the Secretary relating to the use of cyber opposition forces. Each agreement shall require the command—

''(1) to support a high state of mission readiness in the command through the use of one or more cyber opposition forces in continuous exercises and other training activities as considered appropriate by the commander of the command; and

''(2) in conducting such exercises and training activities, [to] meet the standard required under subsection (b).

''(b) JOINT STANDARD FOR CYBER OPPOSITION FORCES.—Not later than March 31, 2017, the Secretary of Defense shall issue a joint training and certification

standard for use by all cyber opposition forces within the Department of Defense.

''(c) JOINT STANDARD FOR PROTECTION OF CONTROL SYSTEMS.—Not later than June 30, 2017, the Secretary of Defense shall issue a joint training and certification standard for the protection of control systems for use by all cyber operations forces within the Department of Defense. Such standard shall—

''(1) provide for applied training and exercise capabilities; and

''(2) use expertise and capabilities from other departments and agencies of the Federal Government, as appropriate.

''(d) BRIEFING REQUIRED.—Not later than September 30, 2017, the Secretary of Defense shall provide to the Committees on Armed Services of the Senate and the House of Representatives a briefing that includes—

''(1) a list of each combatant command that has established an agreement under subsection (a);

''(2) with respect to each such agreement—

''(A) special conditions in the agreement placed on any cyber opposition force used by the command;

''(B) the process for making decisions about deconfliction and risk mitigation of cyber opposition force activities in continuous exercises and training;

''(C) identification of cyber opposition forces trained and certified to operate at the joint standard, as issued under subsection (b);

''(D) identification of the annual exercises that will include participation of the cyber opposition forces; and

''(E) identification of any shortfalls in resources that may prevent annual exercises using cyber opposition forces; and

''(3) any other matters the Secretary of Defense considers appropriate.''

CYBER PROTECTION SUPPORT FOR DEPARTMENT OF DEFENSE PERSONNEL IN POSITIONS HIGHLY VULNERABLE TO CYBER ATTACK

Pub. L. 114–328, div. A, title XVI, §1645, Dec. 23, 2016, 130 Stat. 2603, provided that:

''(a) AUTHORITY TO PROVIDE CYBER PROTECTION SUPPORT.—

''(1) IN GENERAL.—Subject to a determination by the Secretary of Defense, the Secretary may provide cyber protection support for the personal technology devices of the personnel described in paragraph (2).

''(2) AT-RISK PERSONNEL.—The personnel described in this paragraph are personnel of the Department of Defense—

''(A) who the Secretary determines to be highly vulnerable to cyber attacks and hostile information collection activities because of the positions occupied by such personnel in the Department; and

''(B) whose personal technology devices are highly vulnerable to cyber attacks and hostile information collection activities.

''(b) NATURE OF CYBER PROTECTION SUPPORT.—Subject to the availability of resources, the cyber protection support provided to personnel under subsection (a) may include training, advice, assistance, and other services relating to cyber attacks and hostile information collection activities.

''(c) LIMITATION ON SUPPORT.—Nothing in this section shall be construed—

''(1) to encourage personnel of the Department of Defense to use personal technology devices for official business; or

''(2) to authorize cyber protection support for senior Department personnel using personal devices and networks in an official capacity.

''(d) REPORT.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2016], the Secretary shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report on the provision of cyber protection support under subsection (a). The report shall include—

''(1) a description of the methodology used to make the determination under subsection (a)(2); and

''(2) guidance for the use of cyber protection support and tracking of support requests for personnel receiving cyber protection support under subsection (a).

''(e) PERSONAL TECHNOLOGY DEVICES DEFINED.—In this section, the term 'personal technology devices' means technology devices used by Department of Defense personnel outside of the scope of their employment with the Department and includes networks to which such devices connect.''

LIMITATION ON FULL DEPLOYMENT OF JOINT REGIONAL SECURITY STACKS

Pub. L. 114–328, div. A, title XVI, §1646, Dec. 23, 2016, 130 Stat. 2604, provided that:

''(a) LIMITATION.—The Secretary of a military department or the head of a Defense Agency may not declare that such department or Defense Agency has achieved full operational capability for the deployment of joint regional security stacks until the date on which—

''(1) the department or Defense Agency concerned completes operational test and evaluation activities to determine the effectiveness, suitability, and survivability of the joint regional security stacks system of such department or Defense Agency; and

''(2) written certification that such testing and evaluation activities have been completed is provided to the Secretary of such department or the head of such Defense Agency by the appropriate operational test and evaluation organization of such department or Defense Agency.

''(b) WAIVER.—

''(1) IN GENERAL.—The Secretary of a military department or the head of a Defense Agency may waive the requirements of subsection (a) if a certification described in paragraph (2) is provided to the Secretary of Defense, and signed by—

''(A) the Secretary of the military department or the head of the Defense Agency concerned;

''(B) the Director of Operational Test and Evaluation for the Department of Defense; and

''(C) the Chief Information Officer of the Department of Defense.

''(2) CERTIFICATION.—A certification described in this subsection is a written certification that—

''(A) the testing and evaluation activities required under subsection (a) are unnecessary, accompanied by an explanation of the reasons such activities are unnecessary;

''(B) the effectiveness, suitability, and survivability of the joint regional security stacks system of the military department or Defense Agency concerned has been demonstrated by methods other than the testing and evaluation activities required under subsection (a), accompanied by supporting data; or

''(C) national security needs justify full deployment of the joint regional security stacks system of the military department or Defense Agency concerned before the test and evaluation activities required under subsection (a) can be completed, accompanied by an explanation of such justification and a risk management plan.''

EVALUATION OF CYBER VULNERABILITIES OF DEPARTMENT OF DEFENSE CRITICAL INFRASTRUCTURE

Pub. L. 114–328, div. A, title XVI, §1650, Dec. 23, 2016, 130 Stat. 2607, as amended by Pub. L. 115–91, div. A, title XVI, §1643, Dec. 12, 2017, 131 Stat. 1748; Pub. L. 115–232, div. A, title XVI, §1634, Aug. 13, 2018, 132 Stat. 2125, provided that:

''(a) PLAN FOR EVALUATION.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2016], the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Rep-

resentatives] a plan for the evaluation of the cyber vulnerabilities of the critical infrastructure of the Department of Defense.

''(2) ELEMENTS.—The plan under paragraph (1) shall include—

''(A) an identification of each of the military installations to be evaluated; and

''(B) an estimate of the cost of the evaluation.

''(3) PRIORITY IN EVALUATION.—The plan under paragraph (1) shall prioritize the evaluation of military installations based on the criticality of the infrastructure supporting such installations, as determined by the Chairman of the Joint Chiefs of Staff based on an assessment of—

''(A) the Armed Forces stationed at such military installations; and

''(B) threats to such military installations.

''(4) INTEGRATION WITH OTHER EFFORTS.—The plan under paragraph (1) shall build upon other efforts of Department of Defense relating to the identification and mitigation of cyber vulnerabilities of major weapon systems and critical infrastructure of the Department and shall not duplicate such efforts.

''(b) PILOT PROGRAM.—

''(1) IN GENERAL.—Not later than 30 days after the date on which the Secretary submits the plan under subsection (a), the Secretary, acting through a covered research laboratory and the Defense Digital Service, shall initiate a pilot program under which the Secretary shall assess the feasibility and advisability of applying new, innovative methodologies or engineering approaches—

''(A) to improve the defense of control systems against cyber attacks;

''(B) to increase the resilience of military installations against cybersecurity threats;

''(C) to prevent or mitigate the potential for high-consequence cyber attacks;

''(D) to inform future requirements for the development of such control systems; and

''(E) to assess the strategic benefits derived from, and the challenges associated with, isolating military infrastructure from the national electric grid and the use of microgrids.

''(2) LOCATIONS.—The Secretary shall carry out the pilot program under paragraph (1) at not fewer than two military installations selected by the Secretary from among military installations that support the most critical mission-essential functions of the Department of Defense as identified in the plan under subsection (a).

''(3) TOOLS.—In carrying out the pilot program under paragraph (1), the Secretary may use tools and solutions developed under subsection (e).

''(4) REPORT.—Not later than December 31, 2020, the Secretary shall submit to the congressional defense committees a final report on the pilot program that includes—

''(A) a description of the activities carried out under the pilot program at each military installation concerned;

''(B) an assessment of the value of the methodologies or tools applied during the pilot program in increasing the resilience of military installations against cybersecurity threats;

''(C) recommendations for administrative or legislative actions to improve the ability of the Department to employ methodologies and tools for reducing cyber vulnerabilities in other activities of the Department of Defense; and

''(D) recommendations for including such methodologies or tools as requirements for relevant activities, including technical requirements for systems or military construction projects.

''(5) TERMINATION.—The authority of the Secretary to carry out the pilot program under this subsection shall terminate on September 30, 2020.

''(c) EVALUATION.—

''(1) IN GENERAL.—Not later than December 31, 2020, the Secretary shall complete an evaluation of the cyber vulnerabilities of the critical infrastructure of the Department of Defense in accordance with the plan under subsection (a).

''(2) RISK MITIGATION STRATEGIES.—The Secretary shall develop strategies for mitigating the risks of cyber vulnerabilities identified in the course of the evaluation under paragraph (1).

''(d) STATUS ON PROGRESS.—The Secretary shall include in each quarterly cyber operations briefing submitted to Congress under section 484 of title 10, United States Code, a summary of any activities carried out as part of—

''(1) the pilot program under subsection (b); or

''(2) the evaluation under subsection (c).

''(e) TOOLS AND SOLUTIONS.—The Secretary may—

''(1) develop tools that improve assessments of cyber vulnerabilities of Department of Defense critical infrastructure;

''(2) conduct non-recurring engineering for the design of mitigation solutions for such vulnerabilities; and

''(3) establish Department-wide information repositories to share findings relating to such assessments and to share such mitigation solutions.

''(f) DEFINITIONS.—In this section:

''(1) CRITICAL INFRASTRUCTURE OF THE DEPARTMENT OF DEFENSE.—The term 'critical infrastructure of the Department of Defense' means any asset of the Department of Defense of such extraordinary importance to the functioning of the Department and the operation of the Armed Forces that the incapacitation or destruction of such asset by a cyber attack would have a debilitating effect on the ability of the Department to fulfill its missions.

''(2) COVERED RESEARCH LABORATORY.—The term 'covered research laboratory' means—

''(A) a research laboratory of the Department of Defense; or

''(B) a research laboratory of the Department of Energy approved by the Secretary of Energy to carry out the pilot program under subsection (b).''

PLAN FOR INFORMATION SECURITY CONTINUOUS MONITORING CAPABILITY AND COMPLY-TO-CONNECT POLICY; LIMITATION ON SOFTWARE LICENSING

Pub. L. 114–328, div. A, title XVI, § 1653, Dec. 23, 2016, 130 Stat. 2610, provided that:

''(a) INFORMATION SECURITY MONITORING PLAN AND POLICY.—

''(1) PLAN AND POLICY.—The Chief Information Officer of the Department of Defense and the Commander of the United States Cyber Command shall jointly develop—

''(A) a plan for a modernized, Department-wide automated information security continuous monitoring capability that includes—

''(i) a proposed information security architecture for the capability;

''(ii) a concept of operations for the capability; and

''(iii) requirements with respect to the functionality and interoperability of the tools, sensors, systems, processes, and other components of the continuous monitoring capability; and

''(B) a comply-to-connect policy that requires systems to automatically comply with the configurations of the networks of the Department as a condition of connecting to such networks.

''(2) CONSULTATION.—In developing the plan and policy under paragraph (1), the Chief Information Officer and the Commander shall consult with the Principal Cyber Advisor to the Secretary of Defense.

''(3) IMPLEMENTATION.—The Chief Information Officer and the Commander shall each issue such directives as they each consider appropriate to ensure compliance with the plan and policy developed under paragraph (1).

''(4) INCLUSION IN BUDGET MATERIALS.—The Secretary of Defense shall include funding and program plans relating to the plan and policy under paragraph

(1) in the budget materials submitted by the Secretary in support of the budget of the President for fiscal year 2019 (as submitted to Congress under section 1105(a) of title 31, United States Code).

''(5) INTEGRATION WITH OTHER CAPABILITIES.—The Chief Information Officer and the Commander shall ensure that information generated through automated and automation-assisted processes for continuous monitoring, asset management, and comply-to-connect policies and processes shall be accessible and usable in machine-readable form to appropriate cyber protection teams and computer network defense service providers.

''(6) SOFTWARE LICENSE COMPLIANCE MATTERS.—The plan and policy required by paragraph (1) shall comply with the software license inventory requirements of the plan issued pursuant to section 937 of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239; 10 U.S.C. 2223 note) and updated pursuant to section 935 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66; 10 U.S.C. 2223 note).

''(b) LIMITATION ON FUTURE SOFTWARE LICENSING.—

''(1) IN GENERAL.—Subject to paragraph (2), none of the funds authorized to be appropriated by this Act [see Tables for classification] or otherwise made available for fiscal year 2017 or any fiscal year thereafter for the Department of Defense may be obligated or expended on a contract for a software license with a cost of more than $5,000,000 in a fiscal year unless the Department is able, through automated means—

''(A) to count the number of such licenses in use; and

''(B) to determine the security status of each instance of use of the software licensed.

''(2) EFFECTIVE DATE.—Paragraph (1) shall apply—

''(A) beginning on January 1, 2018, with respect to any contract entered into by the Secretary of Defense on or after such date for the licensing of software; and

''(B) beginning on January 1, 2020, with respect to any contract entered into by the Secretary for the licensing of software that was in effect on December 31, 2017.''

ACQUISITION AUTHORITY OF THE COMMANDER OF UNITED STATES CYBER COMMAND

Pub. L. 114–92, div. A, title VIII, §807, Nov. 25, 2015, 129 Stat. 886, as amended by Pub. L. 115–232, div. A, title XVI, §1635, Aug. 13, 2018, 132 Stat. 2125, provided that:

''(a) AUTHORITY.—

''(1) IN GENERAL.—The Commander of the United States Cyber Command shall be responsible for, and shall have the authority to conduct, the following acquisition activities:

''(A) Development and acquisition of cyber operations-peculiar equipment and capabilities.

''(B) Acquisition and sustainment of cyber capability-peculiar equipment, capabilities, and services.

''(2) ACQUISITION FUNCTIONS.—Subject to the authority, direction, and control of the Secretary of Defense, the Commander shall have authority to exercise the functions of the head of an agency under chapter 137 of title 10, United States Code.

''(b) COMMAND ACQUISITION EXECUTIVE.—

''(1) IN GENERAL.—The staff of the Commander shall include a command acquisition executive, who shall be responsible for the overall supervision of acquisition matters for the United States Cyber Command. The command acquisition executive shall have the authority—

''(A) to negotiate memoranda of agreement with the military departments and Department of Defense components to carry out the acquisition of equipment, capabilities, and services described in subsection (a)(1) on behalf of the Command;

''(B) to supervise the acquisition of equipment, capabilities, and services described in subsection (a)(1);

''(C) to represent the Command in discussions with the military departments regarding acquisition programs for which the Command is a customer; and

''(D) to work with the military departments to ensure that the Command is appropriately represented in any joint working group or integrated product team regarding acquisition programs for which the Command is a customer.

''(2) DELIVERY OF ACQUISITION SOLUTIONS.—The command acquisition executive of the United States Cyber Command shall be—

''(A) responsible to the Commander for rapidly delivering acquisition solutions to meet validated cyber operations-peculiar requirements;

''(B) subordinate to the defense acquisition executive in matters of acquisition;

''(C) subject to the same oversight as the service acquisition executives; and

''(D) included on the distribution list for acquisition directives and instructions of the Department of Defense.

''(c) ACQUISITION PERSONNEL.—

''(1) IN GENERAL.—The Secretary of Defense shall provide the United States Cyber Command with the personnel or funding equivalent to ten full-time equivalent personnel to support the Commander in fulfilling the acquisition responsibilities provided for under this section with experience in—

''(A) program acquisition;

''(B) the Joint Capabilities Integration and Development System Process;

''(C) program management;

''(D) system engineering; and

''(E) costing.

''(2) EXISTING PERSONNEL.—The personnel provided under this subsection shall be provided from among the existing personnel of the Department of Defense.

''(d) BUDGET.—In addition to the activities of a combatant command for which funding may be requested under section 166 of title 10, United States Code, the budget proposal of the United States Cyber Command shall include requests for funding for—

''(1) development and acquisition of cyber operations-peculiar equipment; and

''(2) acquisition and sustainment of other capabilities or services that are peculiar to cyber operations activities.

''(e) CYBER OPERATIONS PROCUREMENT FUND.—In exercising the authority granted in subsection (a), the Commander may not obligate or expend more than $75,000,000 out of the funds made available in each fiscal year from 2016 through 2025 to support acquisition activities provided for under this section.

''(f) RULE OF CONSTRUCTION REGARDING INTELLIGENCE AND SPECIAL ACTIVITIES.—Nothing in this section shall be construed to constitute authority to conduct any activity which, if carried out as an intelligence activity by the Department of Defense, would require a notice to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives under title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.).

''(g) IMPLEMENTATION PLAN REQUIRED.—The authority granted in subsection (a) shall become effective 30 days after the date on which the Secretary of Defense provides to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a plan for implementation of those authorities under subsection (a). The plan shall include the following:

''(1) A Department of Defense definition of—

''(A) cyber operations-peculiar equipment and capabilities; and

''(B) cyber capability-peculiar equipment, capabilities, and services.

''(2) Summaries of the components to be negotiated in the memorandum of agreements with the military departments and other Department of Defense components to carry out the development, acquisition,

and sustainment of equipment, capabilities, and services described in subparagraphs (A) and (B) of subsection (a)(1).

''(3) Memorandum of agreement negotiation and approval timelines.

''(4) Plan for oversight of the command acquisition executive established in subsection (b).

''(5) Assessment of the acquisition workforce needs of the United States Cyber Command to support the authority in subsection (a) until 2021.

''(6) Other matters as appropriate.

''(h) ANNUAL END-OF-YEAR ASSESSMENT.—Each year, the Cyber Investment Management Board shall review and assess the acquisition activities of the United States Cyber Command, including contracting and acquisition documentation, for the previous fiscal year, and provide any recommendations or feedback to the acquisition executive of Cyber Command.

''(i) SUNSET.—

''(1) IN GENERAL.—The authority under this section shall terminate on September 30, 2025.

''(2) LIMITATION ON DURATION OF ACQUISITIONS.—The authority under this section does not include major defense acquisition programs, major automated information system programs, or acquisitions of foundational infrastructure or software architectures the duration of which is expected to last more than five years.''

EVALUATION OF CYBER VULNERABILITIES OF MAJOR WEAPON SYSTEMS OF THE DEPARTMENT OF DEFENSE

Pub. L. 114–92, div. A, title XVI, § 1647, Nov. 25, 2015, 129 Stat. 1118, as amended by Pub. L. 114–328, div. A, title XVI, § 1649(b), Dec. 23, 2016, 130 Stat. 2606, provided that:

''(a) EVALUATION REQUIRED.—

''(1) IN GENERAL.—The Secretary of Defense shall, in accordance with the plan under subsection (b), complete an evaluation of the cyber vulnerabilities of each major weapon system of the Department of Defense by not later than December 31, 2019.

''(2) EXCEPTION.—The Secretary may waive the requirement of paragraph (1) with respect to a weapon system or complete the evaluation of a weapon system required by such paragraph after the date specified in such paragraph if the Secretary certifies to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] before that date that all known cyber vulnerabilities in the weapon system have minimal consequences for the capability of the weapon system to meet operational requirements or otherwise satisfy mission requirements.

''(b) PLAN FOR EVALUATION.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Nov. 25, 2015], the Secretary shall submit to the congressional defense committees the plan of the Secretary for the evaluations of major weapon systems under subsection (a), including an identification of each of the weapon systems to be evaluated and an estimate of the funding required to conduct the evaluations.

''(2) PRIORITY IN EVALUATIONS.—The plan under paragraph (1) shall accord a priority among evaluations based on the criticality of major weapon systems, as determined by the Chairman of the Joint Chiefs of Staff based on an assessment of employment of forces and threats.

''(3) INTEGRATION WITH OTHER EFFORTS.—The plan under paragraph (1) shall build upon existing efforts regarding the identification and mitigation of cyber vulnerabilities of major weapon systems, and shall not duplicate similar ongoing efforts such as Task Force Cyber Awakening of the Navy or Task Force Cyber Secure of the Air Force.

''(c) STATUS ON PROGRESS.—The Secretary shall inform the congressional defense committees of the activities undertaken in the evaluation of major weapon systems under this section as part of the quarterly cyber operations briefings under section 484 of title 10, United States Code.

''(d) TOOLS AND SOLUTIONS FOR ASSESSING AND MITIGATING CYBER VULNERABILITIES.—In addition to carrying out the evaluation of cyber vulnerabilities of major weapon systems of the Department under this section, the Secretary may—

''(1) develop tools to improve the detection and evaluation of cyber vulnerabilities;

''(2) conduct non-recurring engineering for the design of solutions to mitigate cyber vulnerabilities; and

''(3) establish Department-wide information repositories to share findings relating to the evaluation and mitigation of cyber vulnerabilities.

''(e) RISK MITIGATION STRATEGIES.—As part of the evaluation of cyber vulnerabilities of major weapon systems of the Department under this section, the Secretary shall develop strategies for mitigating the risks of cyber vulnerabilities identified in the course of such evaluations.

''(f) AUTHORIZATION OF APPROPRIATIONS.—Of the funds authorized to be appropriated by this Act [see Tables for classification] or otherwise made available for fiscal year 2016 for research, development, test, and evaluation, Defense-wide, not more than $200,000,000 shall be available to the Secretary to conduct the evaluations under subsection (a)(1).''

NOTIFICATION OF FOREIGN THREATS TO INFORMATION TECHNOLOGY SYSTEMS IMPACTING NATIONAL SECURITY

Pub. L. 113–291, div. A, title X, § 1078, Dec. 19, 2014, 128 Stat. 3520, provided that:

''(a) NOTIFICATION REQUIRED.—

''(1) IN GENERAL.—Not later than 30 days after the Secretary of Defense determines, through the use of open source information or the use of existing authorities (including section 806 of the National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383; 124 Stat. 4260; 10 U.S.C. 2304 note)), that there is evidence of a national security threat described in paragraph (2), the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a notification of such threat.

''(2) NATIONAL SECURITY THREAT.—A national security threat described in this paragraph is a threat to an information technology or telecommunications component or network by an agent of a foreign power in which the compromise of such technology, component, or network poses a significant risk to the programs and operations of the Department of Defense, as determined by the Secretary of Defense.

''(3) FORM.—A notification under this subsection shall be submitted in classified form.

''(b) ACTION PLAN REQUIRED.—In the event that a notification is submitted pursuant to subsection (a), the Secretary shall work with the head of any department or agency affected by the national security threat to develop a plan of action for responding to the concerns leading to the notification.

''(c) AGENT OF A FOREIGN POWER.—In this section, the term 'agent of a foreign power' has the meaning given such term in section 101(b) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(b)).''

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.''

Pub. L. 114–328, div. A, title XVI, §1643(b), Dec. 23, 2016, 130 Stat. 2602, provided that: ''The Principal Cyber Advisor, acting through the cross-functional team established by section 932(c)(3) of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66; 10 U.S.C. 2224 note) [set out above] and in consultation with the Commander of the United States Cyber Command, shall supervise—

''(1) the development of training standards for computer network operations tool developers for military, civilian, and contractor personnel supporting the cyber mission forces;

''(2) the rapid enhancement of capacity to train personnel to those standards to meet the needs of the cyber mission forces for tool development; and

''(3) actions necessary to ensure timely completion of personnel security investigations and adjudications of security clearances for tool development personnel.''

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, as amended by Pub. L. 114–92, div. A, title II, §231, Nov. 25, 2015, 129 Stat. 778, 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 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 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 during 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 [former] section 3542(b)(2) of title 44, United States Code [see now 44 U.S.C. 3552(b)(6)]; 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, which authorized the Secretary of Defense to establish criteria and reporting procedures applicable to penetration of cleared defense contractors' networks or information systems, was transferred to chapter 19 of this title, redesignated as section 393, and amended by Pub. L. 114–92, div. A, title XVI, §1641(a), Nov. 25, 2015, 129 Stat. 1114.

INSIDER THREAT DETECTION

Pub. L. 112–81, div. A, title IX, §922, Dec. 31, 2011, 125 Stat. 1537, as amended by Pub. L. 114–92, div. A, title X, §1073(e), Nov. 25, 2015, 129 Stat. 996, 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.''

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 [former] section 3542(b)(2) of title 44, United States Code [see now 44 U.S.C. 3552(b)(6)].

''(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[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. Repealed. Pub. L. 114–328, div. A, title VIII, § 833(b)(2)(A), Dec. 23, 2016, 130 Stat. 2284]

Section, 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, related to tracking and management of information technology purchases.

TIME FOR IMPLEMENTATION; APPLICABILITY

Pub. L. 106–398, §1 [[div. A], title VIII, §812(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–214, which provided that the Secretary of Defense was to collect data as required under section 2225 of this title for all contractual ac-

[1] See References in Text note below.