compliance of that infrastructure with such policies, procedures, and practices, including automation of—

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

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

''(b) DEFINITIONS.—In this section:

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

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

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

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

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

[§ 2223a. Renumbered § 4571]

§ 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.)

Editorial Notes

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).

Statutory Notes and Related Subsidiaries

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.

USABILITY OF ANTIQUATED AND PROPRIETARY DATA FORMATS FOR MODERN OPERATIONS

Pub. L. 118–159, div. A, title XV, §1521, Dec. 23, 2024, 138 Stat. 2138, provided that:

''(a) STRATEGY AND ROADMAP.—

''(1) IN GENERAL.—Not later than 270 days after the date of enactment of this Act [Dec. 23, 2024], the Secretary of Defense, in coordination with the Secretaries of the military departments, shall develop—

''(A) a strategy for the Department of Defense, including each of the military departments, to identify, implement, and use modern data formats as the primary method of electronic communication for command and control activities and for weapon systems, including sensors associated with such weapon systems; and

''(B) an associated five-year roadmap for the Department of Defense, including each of the military departments, to implement modern data formats under the strategy described in subparagraph (A).

''(2) ELEMENTS.—The strategy and roadmap required under paragraph (1) shall include the following elements:

''(A) The activities of the Chief Digital and Artificial Intelligence Officer of the Department of Defense to increase and synchronize the use of modern data formats and modern data sharing standards across the Department of Defense.

''(B) Development of standard definitions for modern and antiquated data formats, including a representative catalog of the types of data formats that fall under each category.

''(C) The activities of the military departments to increase the use of modern data formats and modern data sharing standards for command and control systems, weapon systems, and sensors associated with such weapon systems.

''(D) An identification of barriers to the use of modern data formats and modern data sharing standards within weapon systems and sensors associated with such weapon systems across the Department of Defense.

''(E) An identification of barriers to the use of modern data formats and modern data sharing standards within command and control systems across the Department of Defense.

''(F) An identification of limitations on combined joint all-domain command and control capabilities resulting from the use of antiquated data formats.

''(G) An identification of policy documents, instructions, or other guidance requiring an update pursuant to such strategy.

''(H) The sources of funding for each military department with respect to implementation of such strategy.

''(3) SUBMISSION TO CONGRESS.—Upon completion of the strategy and roadmap required under this subsection, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives such strategy.

''(4) MODERN DATA FORMATS.—For the purposes of this subsection, the term 'modern data formats' includes—

''(A) the JavaScript Object Notation data format;

''(B) the Binary JavaScript Object Notation data format;

''(C) the Protocol Buffers data format; and

''(D) such other data formats that the Secretary of Defense determines would meet the requirements in this section.

''(b) PILOT PROGRAMS.—

''(1) ESTABLISHMENT.—Not later than 60 days after the completion of the strategy required by subsection (a)—

''(A) the Secretary of Defense shall establish a pilot program under which the Department of Defense, other than the military departments, shall use modern data formats to improve the usability and functionality of information stored or produced in antiquated data formats, including by the automated conversion of such information to modern data formats; and

''(B) each Secretary of a military department shall establish a pilot program under which such military department shall use modern data formats as described in subparagraph (A).

''(2) BRIEFING.—Not later than 180 days after the completion of the strategy required by subsection (a), the Secretary of Defense and the Secretaries of the military departments shall each submit to the Committees on Armed Services of the Senate and the House of Representatives a briefing on the progress of the pilot program established by such Secretary under this subsection, including specific examples of the use of modern data formats under such pilot program to improve the usability and functionality of information stored or produced in antiquated data formats.

''(3) SUNSET.—Each pilot program established under this subsection shall terminate on the date that is five years after the date of the enactment of this Act.

''(c) MILITARY DEPARTMENT DEFINED.—In this section, the term 'military department' has the meaning given such term in section 101(a) of title 10, United States Code.''

UPDATE OF BIOMETRIC POLICY OF DEPARTMENT OF DEFENSE

Pub. L. 118–159, div. A, title XV, §1523, Dec. 23, 2024, 138 Stat. 2142, provided that:

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2024], the Under Secretary of Defense for Intelligence and Security shall update the policy of the Department of Defense regarding the protection of biometric data.

''(b) ELEMENTS.—The policy updates required by subsection (a) shall include the following:

''(1) Standards for encrypting and protecting data on biometric collection devices.

''(2) A requirement to sanitize biometric data from collection devices and hard drives prior to disposal of the devices and hard drives.

''(3) A requirement that components of the Department maintain records that they have sanitized all data from biometric collection devices when the devices are turned in for disposal.''

REVIEW AND PLAN RELATING TO CYBER RED TEAMS OF DEPARTMENT OF DEFENSE

Pub. L. 118–31, div. A, title XV, § 1507, Dec. 22, 2023, 137 Stat. 540, provided that:

''(a) REVIEW RELATING TO PRIOR JOINT ASSESSMENT.—

''(1) REVIEW REQUIRED.—Not later than 90 days after the date of the enactment of this Act [Dec. 22, 2023], the officials described in subsection (c) shall review, and assess the status of the implementation of, the recommendations set forth by the Secretary of Defense in response to the joint assessment requirement under section 1660 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 133 Stat. 1771).

''(2) ELEMENTS.—The review under paragraph (1) shall include, with respect to the recommendations specified in such paragraph—

''(A) the timelines associated with each such recommendation, regardless of whether the recommendation is fully implemented or yet to be fully implemented; and

''(B) a description of any impediments to the implementation of such recommendations encountered.

''(b) PLAN REQUIRED.—

''(1) PLAN.—Not later than 180 days after the date of the enactment of this Act, the officials described in subsection (c) shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a plan, developed taking into account the findings of the review under subsection (a), to ensure cyber red teams of the Department of Defense achieve sufficient capacity and capability to provide services and meet current and projected future demands on a Defense-wide basis. Such plan shall include—

''(A) a description of the funding necessary for such cyber red teams to achieve such capacity and capability;

''(B) a description of any other resources, personnel, infrastructure, or authorities for access to information necessary for such cyber red teams to achieve such capacity and capability (including with respect to the emulation of threats from foreign countries with advanced cyber capabilities, automation, artificial intelligence or machine learning, and data collection and correlation); and

''(C) updated joint service standards and metrics to ensure the training, staffing, and equipping of such cyber red teams at levels necessary to achieve such capacity and capability.

''(2) IMPLEMENTATION.—Not later than one year after the date of enactment of this Act, the Secretary of Defense shall prescribe such regulations and issue such guidance as the Secretary determines necessary to implement the plan developed under subsection (a).

''(c) OFFICIALS DESCRIBED.—The officials described in this subsection are the Principal Cyber Advisor to the Secretary of Defense, the Chief Information Officer of the Department of Defense, the Director of Operational Test and Evaluation, and the Commander of the United States Cyber Command.

''(d) ANNUAL REPORTS.—Not later than January 31, 2025, and not less frequently than annually thereafter until January 31, 2031, the Director of Operational Test and Evaluation shall include in each annual report required under section 139(h) of title 10, United States Code, an update on progress made with respect to the implementation of this section, including the following:

''(1) The results of test and evaluation events, including any resource or capability shortfalls limiting the capacity or capability of cyber red teams of the Department of Defense to meet operational requirements.

''(2) The extent to which operations of such cyber red teams have expanded across the competition continuum, including during cooperation and competition phases, to match adversary positioning and cyber activities.

''(3) A summary of identified categories of common gaps and shortfalls across cyber red teams of the military departments and Defense Agencies (as such terms are defined in section 101 of title 10, United States Code).

''(4) Any identified lessons learned that would affect training or operational employment decisions relating to the cyber red teams of the Department of Defense.''

TRANSFER OF DATA AND TECHNOLOGY DEVELOPED UNDER MOSAICS PROGRAM

Pub. L. 118–31, div. A, title XV, § 1514, Dec. 22, 2023, 137 Stat. 545, provided that:

''(a) TRANSFERS AUTHORIZED.—The Secretary of Defense may transfer to eligible private sector entities data and technology developed under the MOSAICS program to enhance cyber threat detection and protection of critical industrial control system assets used for electricity distribution.

''(b) AGREEMENTS.—In carrying out subsection (a), the Secretary of Defense may—

''(1) enter into cooperative research and development agreements under section 4026 of title 10, United States Code; and

''(2) use such other mechanisms for the transfer of technology and data as are authorized by law.

''(c) [sic; there are two subsecs. (c)] NOTIFICATION.—Not later than 15 days after any date on which the Secretary determines to transfer data or technology to an eligible private sector entity under subsection (a), the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a written notification of such determination. Such notification shall include the following:

''(1) An identification of the data or technology to be transferred.

''(2) An identification of the eligible private sector entity, including an identification of the specific individual employed by or otherwise associated with such entity responsible for the security and integrity of the data or technology to be received.

''(3) A detailed description of any special security handling instructions required pursuant to an agreement entered into between the Secretary and the eligible private sector entity for such transfer.

''(4) Timelines associated with such transfer.

''(c) [sic] DEFINITIONS.—In this section:

''(1) The term 'eligible private sector entity' means a private sector entity that—

''(A) has functions relevant to the civil electricity sector; and

''(B) is determined by the Secretary of Defense to be eligible to receive data and technology transferred under subsection (a).

''(2) The term 'MOSAICS program' means the program of the Department of Defense known as the 'More Situational Awareness for Industrial Control Systems Joint Capabilities Technology Demonstration program', or successor program.''

MODERNIZATION PROGRAM FOR NETWORK BOUNDARY AND CROSS-DOMAIN DEFENSE

Pub. L. 118–31, div. A, title XV, § 1515, Dec. 22, 2023, 137 Stat. 546, provided that:

''(a) MODERNIZATION PROGRAM REQUIRED.—The Secretary of Defense shall carry out a modernization program for network boundary and cross-domain defense against cyber attacks. In carrying out such modernization program, the Secretary shall expand upon the fiscal year 2023 pilot program on modernized network boundary defense capabilities and the initial deployment of such capabilities to the primary Internet access points of the Department of Defense managed by the Director of the Defense Information Systems Agency.

''(b) PROGRAM PHASES.—

''(1) IN GENERAL.—The Secretary of Defense shall implement the modernization program under subsection (a) in phases, with the objective of completing such program by October 1, 2028.

''(2) OBJECTIVES.—The phases required by paragraph (1) shall include the following objectives:

''(A) By September 30, 2026, completion of—

''(i) the pilot program specified in subsection (a) and the deployment of modernized network boundary defense capabilities to the Internet access points managed by the Director of the Defense Information Systems Agency; and

''(ii) the extension of modernized network boundary defense capabilities to all additional Internet access points of the information network of the Department of Defense.

''(B) By September 30, 2027, the conduct of a survey, completion of a pilot program, and deployment of modernized network boundary defense capabilities to the access points and cross-domain capabilities of the Secret Internet Protocol Router Network.

''(C) By September 30, 2028, the conduct of a survey, completion of a pilot program, and deployment of modernized network boundary defense capabilities to any remaining classified network or enclave of the information network of the Department.

''(c) IMPLEMENTATION PLAN.—Not later than 90 days after the date of the enactment of this Act [Dec. 22, 2023], the Secretary 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 implementation of the modernization program under subsection (a). Such plan shall include—

''(1) a summary of findings from the pilot program specified in subsection (a); and

''(2) an identification of the resources necessary for such implementation, including for implementing the phase of the modernization program specified in subsection (b)(2)(C).''

ESTABLISHMENT OF CERTAIN IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT ACTIVITIES AS PROGRAM OF RECORD

Pub. L. 118–31, div. A, title XV, § 1516, Dec. 22, 2023, 137 Stat. 546, provided that:

''(a) ESTABLISHMENT OF PROGRAM OF RECORD.—

''(1) PROGRAM OF RECORD.—Except as provided in subsection (b), not later than 120 days after the date of the enactment of this Act [Dec. 22, 2023], the Secretary of Defense shall establish a program of record, governed by standard Department of Defense requirements and practices, and transition all covered activities to such program of record.

''(2) OBJECTIVES.—The program of record under subsection (a) shall include, at a minimum, covered activities undertaken to achieve the following objectives:

''(A) Correcting weaknesses in authentication and credentialing security, including with respect to the program of the Department of Defense known as the 'Public Key Infrastructure' program (or any successor program), identified by the Director of Operational Test and Evaluation in a report submitted to Congress in April, 2023, titled 'FY14–21 Observations of the Compromise of Cyber Credentials'.

''(B) Implementing improved authentication technologies, such as biometric and behavioral authentication techniques and other non-password-based solutions.

''(3) BRIEFING.—Not later than 150 days after the date of the enactment of this Act, the Secretary of Defense shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the covered activities to be included under the program of record under subsection (a).

''(b) WAIVER AUTHORITY.—

''(1) AUTHORITY.—The Secretary of Defense may waive the requirement under subsection (a) if the Secretary of Defense determines that the objectives listed in paragraph (2) of such subsection would be better achieved, and the level of rigor of the operational testing and oversight requirements applicable to such objectives would be improved, through a management approach other than the establishment of a program of record and transition of covered activities to such program of record.

''(2) JUSTIFICATION.—Not later than 14 days after issuing a waiver under paragraph (1), the Secretary of Defense shall submit to the congressional defense committees a detailed justification for the waiver, including—

''(A) an explanation of why the establishment of a program of record is not the preferred approach to achieve the objectives listed in subsection (a)(2);

''(B) details relating to the management approach proposed to be implemented in lieu of the establishment of a program of record;

''(C) an implementation plan for such proposed alternative approach; and

''(D) such other information as the Secretary of Defense determines appropriate.

''(c) DESIGNATION OF DATA ATTRIBUTES.—Not later than 120 days after the date of the enactment of this Act, the Chief Information Officer of the Department of Defense, in coordination with the Secretaries of the military departments, shall complete the designation of Tier 1 level data attributes to be used as a baseline set of standardized attributes for identity, credential, and access management, Defense-wide.

''(d) BRIEFING.—Upon completing the requirement under subsection (c), the Chief Information Officer of the Department of Defense and the Secretaries of the military departments shall provide to the Committees on Armed Services of the House of Representatives and the Senate a briefing on the activities carried out under this section.

''(e) DEFINITIONS.—In this section:

''(1) The term 'covered activity' means any activity of the Office of the Secretary of Defense or a Defense Agency relating to the identity, credential, and access management initiative of the Department of Defense.

''(2) The term 'Defense Agency' has the meaning given that term in section 101 of title 10, United States Code.''

PILOT PROGRAM ON ASSURING CRITICAL INFRASTRUCTURE SUPPORT FOR MILITARY CONTINGENCIES

Pub. L. 118–31, div. A, title XV, § 1517, Dec. 22, 2023, 137 Stat. 548, provided that:

''(a) ESTABLISHMENT OF PILOT PROGRAM.—Not later than 60 days after the date of the enactment of this Act [Dec. 22, 2023], the Secretary of Defense shall establish a pilot program to be known as the 'Assuring Critical Infrastructure Support for Military Contingencies Pilot Program'.

''(b) SELECTION OF INSTALLATIONS.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense, acting through the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs, shall select not fewer than four geographically diverse military installations at which to carry out the pilot program under subsection (a).

''(2) PRIORITIZATION.—

''(A) IN GENERAL.—In selecting military installations under paragraph (1), the Secretary of Defense shall give priority to any military installation that the Secretary determines is a key component of not fewer than two contingency plans or operational plans, with further priority given to such plans in the area of responsibility of the United States Indo-Pacific Command or the United States European Command.

''(B) SELECTION BETWEEN EQUAL PRIORITIES.—If two or more military installations qualify for equal

priority under subparagraph (A), the Secretary of Defense shall give further priority for selection under such paragraph to any such military installation that the Secretary of Defense determines is—

''(i) connected to national-level infrastructure;

''(ii) located near a commercial port; or

''(iii) located near a national financial hub.

''(c) ACTIVITIES.—In carrying out the pilot program under subsection (a), the Secretary of Defense, acting through the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs, shall—

''(1) without duplicating or disrupting existing cyber exercise activities under the National Cyber Exercise Program under section 2220B of the Homeland Security Act of 2002 (6 U.S.C. 665h), conduct cyber resiliency and reconstitution stress test scenarios through tabletop exercises and, if possible, live exercises—

''(A) to assess how to prioritize restoration of power, water, and telecommunications for a military installation in the event of a significant cyberattack on regional critical infrastructure that has similar impacts on State and local infrastructure; and

''(B) to determine the recovery process needed to ensure the military installation has the capability to function and support an overseas contingency operation or a homeland defense mission, as appropriate;

''(2) map dependencies on power, water, and telecommunications at the military installation and the connections to distribution and generation outside the military installation;

''(3) recommend priorities for the order of recovery for the military installation in the event of a significant cyberattack, considering both the requirements needed for operations of the military installation and the potential participation of personnel at the military installation in an overseas contingency operation or a homeland defense mission; and

''(4) develop a lessons-learned database from the exercises conducted under paragraph (1) across all military installations participating in the pilot program, to be shared with the Committees on Armed Services of the House of Representatives and the Senate.

''(d) COORDINATION WITH RELATED PROGRAMS.—The Secretary of Defense, acting through the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs, shall ensure that activities under subsection (c) are coordinated with—

''(1) private entities that operate power, water, and telecommunications for a military installation participating in the pilot program under subsection (a);

''(2) relevant military and civilian personnel; and

''(3) any other entity that the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs determines is relevant to the execution of activities under subsection (c).

''(e) REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall submit to the Assistant to the President for Homeland Security, the National Cyber Director, the head of any other relevant Sector Risk Management Agency, the Committees on Armed Services of the House of Representatives and the Senate, and, if the Secretary of Defense determines it appropriate, relevant private sector owners and operators of critical infrastructure a report on the activities carried out under pilot program under subsection (a), including a description of any operational challenges identified.

''(f) DEFINITIONS.—In this section:

''(1) The term 'critical infrastructure' has the meaning given that term in the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c).

''(2) The term 'Sector Risk Management Agency' has the meaning given that term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).''

REQUIREMENTS FOR IMPLEMENTATION OF USER ACTIVITY MONITORING FOR CERTAIN PERSONNEL

Pub. L. 118–31, div. A, title XV, §1537, Dec. 22, 2023, 137 Stat. 570, provided that:

''(a) IN GENERAL.—The Secretary of Defense shall require each head of a component of the Department of Defense to fully implement each directive, policy, and program requirement for user activity monitoring and least privilege access controls with respect to the personnel of that component, including Federal employees and contractors, granted access to classified information and classified networks, including the following directives (and any successor directives):

''(1) The Committee on National Security Systems Directive 504, issued on February 4, 2014, relating to the protection of national security systems from insider threats (including any annex to such directive).

''(2) Department of Defense Directive 5205.16, issued on September 30, 2014, relating to the insider threat program of the Department of Defense.

''(b) ADDITIONAL REQUIREMENT.—The Secretary of Defense shall require each head of a component of the Department of Defense to implement, with respect to systems, devices, and personnel of the component, automated controls to detect and prohibit privileged user accounts from performing general user activities not requiring privileged access.

''(c) PERIODIC TESTING.—The Secretary shall require that, not less frequently than once every two years, each head of a component of the Department of Defense—

''(1) conducts insider threat testing using threat-realistic tactics, techniques, and procedures; and

''(2) submits to the Under Secretary of Defense for Intelligence and Security, the Chief Information Officer of the Department of Defense, and the Director of Operational Test and Evaluation of the Department of Defense a report on the findings of the head with respect to the testing conducted pursuant to paragraph (1).

''(d) REPORT.—Not later than 180 days after the date of the enactment of this Act [Dec. 22, 2023], the Secretary of Defense shall submit to the appropriate congressional committees a report on the implementation of this section.

''(e) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term 'appropriate congressional committees' means—

''(1) the Committee on Armed Services and the Permanent Select Committee on Intelligence of the House of Representatives; and

''(2) the Committee on Armed Services and the Select Committee on Intelligence of the Senate.''

MANAGEMENT BY DEPARTMENT OF DEFENSE OF MOBILE APPLICATIONS

Pub. L. 118–31, div. A, title XV, §1552, Dec. 22, 2023, 137 Stat. 579, provided that:

''(a) IMPLEMENTATION OF RECOMMENDATIONS.—

''(1) IN GENERAL.—The Secretary of Defense shall evaluate and implement to the maximum extent practicable the recommendations of the Inspector General of the Department of Defense with respect to managing mobile applications contained in the report set forth by the Inspector General dated February 9, 2023, and titled 'Management Advisory: The DoD's Use of Mobile Applications' (Report No. DODIG–2023–041).

''(2) DEADLINE.—The Secretary shall implement each of the recommendations specified in subsection (a) by not later than one year after the date of the enactment of this Act [Dec. 22, 2023] unless the Secretary submits to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a written notification of any specific recommendation that the Secretary declines to implement or plans to implement after the date that is one year after the date of the enactment of this Act.

''(b) BRIEFING ON REQUIREMENTS RELATED TO COVERED APPLICATIONS.—

''(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Secretary shall provide to the congressional defense committees a

briefing on actions taken by the Secretary to enforce compliance with existing policy of the Department of Defense that prohibits—

''(A) the installation and use of covered applications on Federal Government devices; and

''(B) the use of covered applications on the Department of Defense Information Network on personal devices.

''(2) COVERED APPLICATIONS DEFINED.—In this subsection, the term 'covered applications' means the social networking service TikTok, or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.''

ACTIONS TO ADDRESS SERIOUS DEFICIENCIES IN ELECTRONIC PROTECTION OF SYSTEMS THAT OPERATE IN THE RADIO FREQUENCY SPECTRUM

Pub. L. 118–31, div. A, title XVI, § 1686, Dec. 22, 2023, 137 Stat. 620, provided that:

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

''(1) establish requirements for and assign sufficient priority to ensuring electronic protection of military sensor, navigation, and communications systems and subsystems against jamming, spoofing, and unintended interference from military systems of the United States and foreign adversaries; and

''(2) provide management oversight and supervision of the military departments to ensure military systems that emit and receive radio frequencies are protected against threats and interference from United States and foreign adversary military systems operating in the same or adjacent radio frequencies.

''(b) SPECIFIC REQUIRED ACTIONS.—The Secretary of Defense shall require the military departments and combat support agencies to carry out the following activities:

''(1) Not later than 270 days after the date of the enactment of this Act [Dec. 22, 2023], develop and approve requirements, through the Joint Requirements Oversight Council as appropriate, for every radar, signals intelligence, navigation, and communications system and subsystem subject to the Global Force Management process to ensure such systems and subsystems are able to withstand threat-realistic levels of jamming, spoofing, and unintended interference, including self-generated interference.

''(2) Not less frequently than once every 4 years, test each system and subsystem described in paragraph (1) at a test range that permits threat-realistic electronic warfare attacks against the system or subsystem by a red team or simulated opposition force, with the first set of highest priority systems to be initially tested by not later than the end of fiscal year 2025.

''(3) With respect to each system and subsystem described in paragraph (1) that fails to meet electronic protection requirements during testing conducted under paragraph (2)—

''(A) not later than 3 years after the initial failed test, retrofit the system or subsystem with electronic protection measures that can withstand threat-realistic jamming, spoofing, and unintended interference; and

''(B) not later than 4 years after the initial failed test, retest such systems and subsystems.

''(4) Survey, identify, and test available technology that can be practically and affordably retrofitted on the systems and subsystems described in paragraph (1) and which provides robust protection against threat-realistic jamming, spoofing, and unintended interference.

''(5) Design and build electronic protection into ongoing and future development programs to withstand expected jamming and spoofing threats and unintended interference.

''(c) WAIVER.—The Secretary of Defense may establish a process for issuing waivers, on a case-by-case basis, for the testing requirement under paragraph (2) of subsection (b) and for the retrofit requirement under paragraph (3) of such subsection.

''(d) ANNUAL REPORTS.—Concurrent with the submission of the budget of the President to Congress pursuant to section 1105(a) of title 31, United States Code, for each of fiscal years 2025 through 2030, the Director of Operational Test and Evaluation shall submit to the Electronic Warfare Executive Committee of the Department of Defense and the Committees on Armed Services of the Senate and the House of Representatives a comprehensive annual report that—

''(1) aggregates and summarizes information received from the military departments and combat support agencies for purposes of the preparation of the report; and

''(2) includes a description of—

''(A) the activities carried out to implement the requirements of this section;

''(B) the systems and subsystems subject to testing in the previous year and the results of such tests, including a description of the requirements for electronic protection established for the tested systems and subsystems; and

''(C) each waiver issued in the previous year with respect to such requirements, together with a detailed rationale for the waiver and a plan for addressing any issues that formed the basis of the waiver request.''

OPERATIONAL TESTING FOR COMMERCIAL CYBERSECURITY CAPABILITIES

Pub. L. 117–263, div. A, title XV, § 1514, Dec. 23, 2022, 136 Stat. 2895, provided that:

''(a) DEVELOPMENT AND SUBMISSION OF PLANS.—Not later than February 1, 2024, the Chief Information Officer of the Department of Defense and the Chief Information Officers of the military departments shall develop and submit plans described in subsection (b) to the Director of Operational Test and Evaluation who may approve the implementation of the plans pursuant to subsection (c).

''(b) PLANS DESCRIBED.—The plans described in this subsection are plans that—

''(1) ensure covered cybersecurity capabilities are appropriately tested, evaluated, and proven operationally effective, suitable, and survivable prior to operation on a Department of Defense network; and

''(2) specify how test results will be expeditiously provided to the Director of Operational Test and Evaluation.

''(c) ASSESSMENT.—In reviewing the plans submitted under subsection (a), the Director of Operational Test and Evaluation shall conduct an assessment that includes consideration of the following:

''(1) Threat-realistic operational testing, including representative environments, variation of operational conditions, and inclusion of a realistic opposing force.

''(2) The use of Department of Defense cyber red teams, as well as any enabling contract language required to permit threat-representative red team assessments.

''(3) Collaboration with the personnel using the commercial cybersecurity capability regarding the results of the testing to improve operators' ability to recognize and defend against cyberattacks.

''(4) The extent to which additional resources may be needed to remediate any shortfalls in capability to make the commercial cybersecurity capability effective, suitable, and cyber survivable in an operational environment of the Department.

''(5) Identification of training requirements, and changes to training, sustainment practices, or concepts of operation or employment that may be needed to ensure the effectiveness, suitability, and cyber survivability of the commercial cybersecurity capability.

''(d) POLICIES AND REGULATIONS.—Not later than February 1, 2024, the Secretary of Defense shall issue such policies and guidance and prescribe such regulations as the Secretary determines necessary to carry out this section.

''(e) REPORTS.—Not later than January 31, 2025, and not less frequently than annually thereafter until January 31, 2030, the Director shall include in each annual report required by section 139(h) of title 10, United States Code, the following:

''(1) The status of the plans developed under subsection (a).

''(2) The number and type of test and evaluation events completed in the past year for such plans, disaggregated by component of the Department, and including resources devoted to each event.

''(3) The results from such test and evaluation events, including any resource shortfalls affecting the number of commercial cybersecurity capabilities that could be assessed.

''(4) A summary of identified categories of common gaps and shortfalls found during testing.

''(5) The extent to which entities responsible for developing and testing commercial cybersecurity capabilities have responded to recommendations made by the Director in an effort to gain favorable determinations.

''(6) Any identified lessons learned that would impact training, sustainment, or concepts of operation or employment decisions relating to the assessed commercial cybersecurity capabilities.

''(f) DEFINITION.—In this section, the term 'covered cybersecurity capabilities' means any of the following:

''(1) Commercial products (as defined in section 103 of title 41, United States Code) acquired and deployed by the Department of Defense to satisfy the cybersecurity requirements of one or more Department components.

''(2) Commercially available off-the-shelf items (as defined in section 104 of title 41, United States Code) acquired and deployed by the Department of Defense to satisfy the cybersecurity requirements of one or more Department components.

''(3) Noncommercial items acquired through the Adaptive Acquisition Framework and deployed by the Department of Defense to satisfy the cybersecurity requirements of one or more Department components.''

PLAN FOR COMMERCIAL CLOUD TEST AND EVALUATION

Pub. L. 117–263, div. A, title XV, §1553, Dec. 23, 2022, 136 Stat. 2920, provided that:

''(a) POLICY AND PLAN.—Not later than 180 days after the date of enactment of this Act [Dec. 23, 2022], the Secretary of Defense, in consultation with commercial industry, shall implement a policy and plan for test and evaluation of the cybersecurity of the clouds of commercial cloud service providers that provide, or are intended to provide, storage or computing of classified data of the Department of Defense.

''(b) CONTENTS.—The policy and plan under subsection (a) shall include the following:

''(1) A requirement that, beginning on the date of the enactment of this Act, future contracts with cloud service providers for storage or computing of classified data of the Department include provisions that permit the Secretary to conduct independent, threat-realistic assessments of the commercial cloud infrastructure, including with respect to—

''(A) the storage, compute, and enabling elements, including the control plane and virtualization hypervisor for mission elements of the Department supported by the cloud provider; and

''(B) the supporting systems used in the fulfillment, facilitation, or operations relating to the mission of the Department under the contract, including the interfaces with these systems.

''(2) An explanation as to how the Secretary intends to proceed on amending existing contracts with cloud service providers to permit the same level of assessments required for future contracts under paragraph (1).

''(3) Identification and description of any proposed tiered test and evaluation requirements aligned with different impact and classification levels.

''(c) WAIVER AUTHORITY.—The Secretary may include in the policy and plan under subsection (a) an authority to waive any requirement under subsection (b) if the waiver is jointly approved by the Chief Information Officer of the Department of Defense and the Director of Operational Test and Evaluation.

''(d) SUBMISSION.—Not later than 180 days after the date of enactment of this Act, the Secretary shall submit to the Committees on Armed Services of the Senate and the House of Representatives the policy and plan under subsection (a).

''(e) THREAT-REALISTIC ASSESSMENT DEFINED.—In this section, the term 'threat-realistic assessments' means, with respect to commercial cloud infrastructure, activities that—

''(1) are designed to accurately emulate cyber threats from advanced nation state adversaries, such as Russia and China; and

''(2) include cooperative penetration testing and no-notice threat-emulation activities where personnel of the Department of Defense attempt to penetrate and gain control of the cloud-provider facilities, networks, systems, and defenses associated with, or which enable, the supported missions of the Department.''

ASSESSMENTS OF WEAPONS SYSTEMS VULNERABILITIES TO RADIO-FREQUENCY ENABLED CYBER ATTACKS

Pub. L. 117–263, div. A, title XV, §1559, Dec. 23, 2022, 136 Stat. 2926, as amended by Pub. L. 118–31, div. A, title XV, §1502(a)(2)(F), Dec. 22, 2023, 137 Stat. 538, provided that:

''(a) ASSESSMENTS.—The Secretary of Defense shall ensure that the activities required by and conducted pursuant to section 1647 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1118) [10 U.S.C. 2224 note] and the amendments made by section 1712 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283; 134 Stat. 4087 [amending section 1647 of Pub. L. 114–92, set out as a note under this section, and section 1640 of Pub. L. 115–91, formerly set out as a note under this section]) include regular assessments of the vulnerabilities to and mission risks presented by radio-frequency enabled cyber attacks with respect to the operational technology embedded in weapons systems, aircraft, ships, ground vehicles, space systems, sensors, and datalink networks of the Department of Defense.

''(b) ELEMENTS.—The assessments under subsection (a) with respect to vulnerabilities and risks described in such subsection shall include—

''(1) identification of such vulnerabilities and risks;

''(2) ranking of vulnerability, severity, and priority;

''(3) development and selection of options, with associated costs and schedule, to correct such vulnerabilities, including installation of intrusion detection capabilities;

''(4) an evaluation of the cybersecurity sufficiency for Military Standard 1553; and

''(5) development of integrated risk-based plans to implement the corrective actions selected.

''(c) DEVELOPMENT OF CORRECTIVE ACTIONS.—In developing corrective actions under subsection (b)(3), the assessments under subsection (a) shall—

''(1) consider the missions supported by the assessed weapons systems, aircraft, ships, ground vehicles, space systems, sensors, or datalink networks, as the case may be, to ensure that the corrective actions focus on the vulnerabilities that create the greatest risks to the missions;

''(2) be shared and coordinated with the principal staff assistant with primary responsibility for the strategic cybersecurity program; and

''(3) address requirements for deployed and nondeployed members of the Armed Forces to analyze data collected on the weapons systems and respond to attacks.

''(d) INTELLIGENCE INFORMED ASSESSMENTS.—The assessments under subsection (a) shall be informed by in-

telligence, if available, and technical judgment regarding potential threats to embedded operational technology during operations of the Armed Forces.

''(e) COORDINATION.—

''(1) COORDINATION AND INTEGRATION OF ACTIVITIES.—The assessments under subsection (a) shall be fully coordinated and integrated with activities described in such subsection.

''(2) COORDINATION OF ORGANIZATIONS.—The Secretary shall ensure that the organizations conducting the assessments under subsection (a) in the military departments, the United States Special Operations Command, and the Defense Agencies coordinate with each other and share best practices, vulnerability analyses, and technical solutions with the principal staff assistant with primary responsibility for the Strategic Cybersecurity Program.''

COORDINATION BETWEEN UNITED STATES CYBER COMMAND AND PRIVATE SECTOR

Pub. L. 117–81, div. A, title XV, § 1508, Dec. 27, 2021, 135 Stat. 2032, provided that:

''(a) VOLUNTARY PROCESS.—Not later than January 1, 2023, the Commander of United States Cyber Command shall establish a voluntary process to engage with private sector information technology and cybersecurity entities to explore and develop methods and plans through which the capabilities, knowledge, and actions of—

''(1) private sector entities operating inside the United States to defend against foreign malicious cyber actors could assist, or be coordinated with, the actions of United States Cyber Command operating outside the United States against such foreign malicious cyber actors; and

''(2) United States Cyber Command operating outside the United States against foreign malicious cyber actors could assist, or be coordinated with, the actions of private sector entities operating inside the United States against such foreign malicious cyber actors.

''(b) ANNUAL BRIEFING.—

''(1) IN GENERAL.—During the period beginning on March 1, 2022, and ending on March 1, 2026, the Commander of United States Cyber Command shall, not less frequently than once each year, provide to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives a briefing on the status of any activities conducted pursuant to subsection (a).

''(2) ELEMENTS.—Each briefing provided under paragraph (1) shall include the following:

''(A) Such recommendations for legislative or administrative action as the Commander of United States Cyber Command considers appropriate to improve and facilitate the exploration and development of methods and plans under subsection (a).

''(B) Such recommendations as the Commander may have for increasing private sector participation in such exploration and development.

''(C) A description of the challenges encountered in carrying out subsection (a), including any concerns expressed to the Commander by private sector partners regarding participation in such exploration and development.

''(D) Information relating to how such exploration and development with the private sector could assist military planning by United States Cyber Command.

''(E) Such other matters as the Commander considers appropriate.

''(c) CONSULTATION.—In developing the process described in subsection (a), the Commander of United States Cyber Command shall consult with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security and the heads of any other Federal agencies the Commander considers appropriate.

''(d) INTEGRATION WITH OTHER EFFORTS.—The Commander of United States Cyber Command shall ensure that the process described in subsection (a) makes use of, builds upon, and, as appropriate, integrates with and does not duplicate, other efforts of the Department of Homeland Security and the Department of Defense relating to cybersecurity, including the following:

''(1) The Joint Cyber Defense Collaborative of the Cybersecurity and Infrastructure Security Agency.

''(2) The Cybersecurity Collaboration Center and Enduring Security Framework of the National Security Agency.

''(3) The office for joint cyber planning of the Department of Homeland Security.

''(e) PROTECTION OF TRADE SECRETS AND PROPRIETARY INFORMATION.—The Commander of United States Cyber Command shall ensure that any trade secret or proprietary information of a private sector entity engaged with the Department of Defense through the process established under subsection (a) that is made known to the Department pursuant to such process remains private and protected unless otherwise explicitly authorized by such entity.

''(f) RULE OF CONSTRUCTION.—Nothing in this section may be construed to authorize United States Cyber Command to conduct operations inside the United States or for private sector entities to conduct offensive cyber activities outside the United States, except to the extent such operations or activities are permitted by a provision of law in effect on the day before the date of the enactment of this Act [Dec. 27, 2021].''

ENTERPRISE-WIDE PROCUREMENT OF CYBER DATA PRODUCTS AND SERVICES

Pub. L. 117–81, div. A, title XV, § 1521, Dec. 27, 2021, 135 Stat. 2040, as amended by Pub. L. 118–31, div. A, title XV, § 1522, Dec. 22, 2023, 137 Stat. 553; Pub. L. 118–159, div. A, title XV, § 1501, Dec. 23, 2024, 138 Stat. 2131, provided that:

''(a) PROGRAM.—Not later than one year after the date of the enactment of this Act [Dec. 27, 2021], the Secretary of Defense shall designate an executive agent for Department of Defense-wide procurement of cyber data products and services. The executive agent shall establish a program management office responsible for such procurement, and the program manager of such program office shall be responsible for the following:

''(1) Surveying components of the Department for the cyber data products and services needs of such components.

''(2) Conducting market research of cyber data products and services.

''(3) Developing or facilitating development of requirements, both independently and through consultation with components, for the acquisition of cyber data products and services.

''(4) Developing and instituting model contract language for the acquisition of cyber data products and services, including contract language that facilitates components' requirements for ingesting, sharing, using and reusing, structuring, and analyzing data derived from such products and services.

''(5) Conducting procurement of cyber data products and services on behalf of the Department of Defense, including negotiating contracts with a fixed number of licenses based on aggregate component demand and negotiation of extensible contracts.

''(6) Evaluating emerging cyber technologies, such as artificial intelligence-enabled security tools, for efficacy and applicability to the requirements of the Department of Defense.

''(7) Carrying out the responsibilities specified in paragraphs (1) through (6) with respect to the cyber data products and services needs of the Cyberspace Operations Forces, such as cyber data products and services germane to cyberspace topology and identification of adversary threat activity and infrastructure, including—

''(A) facilitating the development of cyber data products and services requirements for the Cyberspace Operations Forces, conducting market research regarding the future cyber data products and

services needs of the Cyberspace Operations Forces, and conducting acquisitions pursuant to such requirements and market research;

''(B) coordinating cyber data products and services acquisition and management activities with Joint Cyber Warfighting Architecture acquisition and management activities, including activities germane to data storage, data management, and development of analytics;

''(C) implementing relevant Department of Defense and United States Cyber Command policy germane to acquisition of cyber data products and services;

''(D) leading or informing the integration of relevant datasets and services, including Government-produced threat data, commercial cyber threat information, collateral telemetry data, topology-relevant data, sensor data, and partner-provided data; and

''(E) facilitating the development of tradecraft and operational workflows based on relevant cyber data products and services.

''(b) COORDINATION.—In implementing this section, each component of the Department of Defense shall coordinate its cyber data products and services requirements and potential procurement plans relating to such products and services with the program management office established pursuant to subsection (a) so as to enable such office to determine if satisfying such requirements or procurement of such products and services on an enterprise-wide basis would serve the best interests of the Department.

''(c) PROHIBITION.—Beginning not later than 540 days after the date of the enactment of this Act, no component of the Department of Defense may independently procure a cyber data product or service that has been procured by the program management office established pursuant to subsection (a), unless—

''(1) such component is able to procure such product or service at a lower per-unit price than that available through such office;

''(2) such office has approved such independent purchase; or

''(3) such component submits to such office a justification for such component to independently procure such product or service that such component determines as demonstrating—

''(A) the compelling need for such product or service; and

''(B) either the urgency for such product or service or the need to ensure competition in the market for such product or service supports such independent procurement by such component.

''(d) EXCEPTION.—United States Cyber Command and the National Security Agency may conduct joint procurements of products and services, including cyber data products and services, except that the requirements of subsections (b) and (c) shall not apply to the National Security Agency.

''(e) DEFINITION.—In this section, the term 'cyber data products and services' means commercially-available datasets and analytic services germane to offensive cyber, defensive cyber, and DODIN operations, including products and services that provide technical data, indicators, and analytic services relating to the targets, infrastructure, tools, and tactics, techniques, and procedures of cyber threats.''

PROTECTIVE DOMAIN NAME SYSTEM WITHIN THE DEPARTMENT OF DEFENSE

Pub. L. 117–81, div. A, title XV, §1524, Dec. 27, 2021, 135 Stat. 2042, provided that:

''(a) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act [Dec. 27, 2021], the Secretary of Defense shall ensure each component of the Department of Defense uses a Protective Domain Name System (PDNS) instantiation offered by the Department.

''(b) EXEMPTIONS.—The Secretary of Defense may exempt a component of the Department from using a PDNS instantiation for any reason except with respect to cost or technical application.

''(c) REPORT TO CONGRESS.—Not later than 150 days after the date of the enactment of this Act, 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 that includes information relating to—

''(1) each component of the Department of Defense that uses a PDNS instantiation offered by the Department;

''(2) each component exempt from using a PDNS instantiation pursuant to subsection (b); and

''(3) efforts to ensure that each PDNS instantiation offered by the Department connects and shares relevant and timely data.''

CYBER DATA MANAGEMENT

Pub. L. 117–81, div. A, title XV, §1527, Dec. 27, 2021, 135 Stat. 2043, provided that:

''(a) IN GENERAL.—The Commander of United States Cyber Command and the Secretaries of the military departments, in coordination with the Principal Cyber Advisor to the Secretary, the Chief Information Officer and the Chief Data Officer of the Department of Defense, and the Chairman of the Joint Chiefs of Staff, shall—

''(1) access, acquire, and use mission-relevant data to support offensive cyber, defensive cyber, and DODIN operations from the intelligence community, other elements of the Department of Defense, and the private sector;

''(2) develop policy, processes, and operating procedures governing the access, ingest, structure, storage, analysis, and combination of mission-relevant data, including—

''(A) intelligence data;

''(B) internet traffic, topology, and activity data;

''(C) cyber threat information;

''(D) Department of Defense Information Network sensor, tool, routing infrastructure, and endpoint data; and

''(E) other data management and analytic platforms pertinent to United States Cyber Command missions that align with the principles of Joint All Domain Command and Control;

''(3) pilot efforts to develop operational workflows and tactics, techniques, and procedures for the operational use of mission-relevant data by the Cyberspace Operations Forces; and

''(4) evaluate data management platforms used to carry out paragraphs (1), (2), and (3) to ensure such platforms operate consistently with the Deputy Secretary of Defense's Data Decrees signed on May 5, 2021.

''(b) ROLES AND RESPONSIBILITIES.—

''(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act [Dec. 27, 2021], the Commander of United States Cyber Command and the Secretaries of the military departments, in coordination with the Principal Cyber Advisor to the Secretary, the Chief Information Officer and Chief Data Officer of the Department of Defense, and the Chairman of the Joint Chiefs of Staff, shall establish the specific roles and responsibilities of the following in implementing each of the tasks required under subsection (a):

''(A) United States Cyber Command.

''(B) Program offices responsible for the components of the Joint Cyber Warfighting Architecture.

''(C) The military services.

''(D) Entities in the Office of the Secretary of Defense.

''(E) Any other program office, headquarters element, or operational component newly instantiated or determined relevant by the Secretary.

''(2) BRIEFING.—Not later than 300 days after the date of the enactment of this Act, the Secretary of Defense shall provide to the congressional defense

committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the roles and responsibilities established under paragraph (1).''

ZERO TRUST STRATEGY, PRINCIPLES, MODEL ARCHITECTURE, AND IMPLEMENTATION PLANS

Pub. L. 118–159, div. A, title XV, § 1513, Dec. 23, 2024, 138 Stat. 2136, provided that:

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2024], the Chief Information Officer of the Department of Defense shall develop guidance for how—

''(1) the zero trust strategy of the Department of Defense developed under section 1528 of the National Defense Authorization Act for Fiscal Year 2022 (10 U.S.C. 2224 note) [set out below] applies to Internet of Things hardware, including human-wearable devices, sensors, and other smart technology used by the United States in military operations; and

''(2) the role identity, credential, and access management technologies serve in enforcing such zero trust strategy.

''(b) INTERNET OF THINGS DEFINED.—In this section, the term 'Internet of Things' has the meaning given such term by the National Institution of Standards and Technology in NIST Special Publication 800-172 and any amendatory or superseding document relating thereto.''

Pub. L. 117–81, div. A, title XV, § 1528, Dec. 27, 2021, 135 Stat. 2044, as amended by Pub. L. 117–263, div. A, title XV, § 1501(c)(2), Dec. 23, 2022, 136 Stat. 2879, provided that:

''(a) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act [Dec. 27, 2021], the Chief Information Officer of the Department of Defense and the Commander of United States Cyber Command shall jointly develop a zero trust strategy, principles, and a model architecture to be implemented across the Department of Defense Information Network, including classified networks, operational technology, and weapon systems.

''(b) STRATEGY, PRINCIPLES, AND MODEL ARCHITECTURE ELEMENTS.—The zero trust strategy, principles, and model architecture required under subsection (a) shall include, at a minimum, the following elements:

''(1) Prioritized policies and procedures for establishing implementations of mature zero trust enabling capabilities within on-premises, hybrid, and pure cloud environments, including access control policies that determine which persona or device shall have access to which resources and the following:

''(A) Identity, credential, and access management.

''(B) Macro and micro network segmentation, whether in virtual, logical, or physical environments.

''(C) Traffic inspection.

''(D) Application security and containment.

''(E) Transmission, ingest, storage, and real-time analysis of cybersecurity metadata endpoints, networks, and storage devices.

''(F) Data management, data rights management, and access controls.

''(G) End-to-end encryption.

''(H) User access and behavioral monitoring, logging, and analysis.

''(I) Data loss detection and prevention methodologies.

''(J) Least privilege, including system or network administrator privileges.

''(K) Endpoint cybersecurity, including secure host, endpoint detection and response, and comply-to-connect requirements.

''(L) Automation and orchestration.

''(M) Configuration management of virtual machines, devices, servers, routers, and similar to be maintained on a single virtual device approved list (VDL).

''(2) Policies specific to operational technology, critical data, infrastructures, weapon systems, and classified networks.

''(3) Specification of enterprise-wide acquisitions of capabilities conducted or to be conducted pursuant to the policies referred to in paragraph (2).

''(4) Specification of standard zero trust principles supporting reference architectures and metrics-based assessment plan.

''(5) Roles, responsibilities, functions, and operational workflows of zero trust cybersecurity architecture and information technology personnel—

''(A) at combatant commands, military services, and defense agencies; and

''(B) Joint Forces Headquarters-Department of Defense Information Network.

''(c) ARCHITECTURE DEVELOPMENT AND IMPLEMENTATION.—In developing and implementing the zero trust strategy, principles, and model architecture required under subsection (a), the Chief Information Officer of the Department of Defense and the Commander of United States Cyber Command shall—

''(1) coordinate with—

''(A) the Principal Cyber Advisor to the Secretary of Defense;

''(B) the Director of the National Security Agency Cybersecurity Directorate;

''(C) the Director of the Defense Advanced Research Projects Agency;

''(D) the Chief Information Officer of each military service;

''(E) the Commanders of the cyber components of the military services;

''(F) the Principal Cyber Advisor of each military service;

''(G) the Chairman of the Joints Chiefs of Staff; and

''(H) any other component of the Department of Defense as determined by the Chief Information Officer and the Commander;

''(2) assess the utility of the Joint Regional Security Stacks, automated continuous endpoint monitoring program, assured compliance assessment solution, and each of the defenses at the Internet Access Points for their relevance and applicability to the zero trust architecture and opportunities for integration or divestment;

''(3) employ all available resources, including online training, leveraging commercially available zero trust training material, and other Federal agency training, where feasible, to implement cybersecurity training on zero trust at the—

''(A) executive level;

''(B) cybersecurity professional or implementer level; and

''(C) general knowledge levels for Department of Defense users;

''(4) facilitate cyber protection team and cybersecurity service provider threat hunting and discovery of novel adversary activity;

''(5) assess and implement means to effect Joint Force Headquarters-Department of Defense Information Network's automated command and control of the entire Department of Defense Information Network;

''(6) assess the potential of and, as appropriate, encourage, use of third-party cybersecurity-as-a-service models;

''(7) engage with and conduct outreach to industry, academia, international partners, and other departments and agencies of the Federal Government on issues relating to deployment of zero trust architectures;

''(8) assess the current Comply-to-Connect Plan; and

''(9) review past and conduct additional pilots to guide development, including—

''(A) utilization of networks designated for testing and accreditation under section 1658 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 10 U.S.C. 2224 note) [set out below];

''(B) use of automated red team products for assessment of pilot architectures; and

''(C) accreditation of piloted cybersecurity products for enterprise use in accordance with the findings on enterprise accreditation standards conducted pursuant to section 1654 of such Act (Public Law 116–92) [133 Stat. 1764].

''(d) IMPLEMENTATION PLANS.—

''(1) IN GENERAL.—Not later than one year after the finalization of the zero trust strategy, principles, and model architecture required under subsection (a), the head of each military department and the head of each component of the Department of Defense shall transmit to the Chief Information Officer of the Department and the Commander of Joint Forces Headquarters-Department of Defense Information Network a draft plan to implement such zero trust strategy, principles, and model architecture across the networks of their respective components and military departments.

''(2) ELEMENTS.—Each implementation plan transmitted pursuant to paragraph (1) shall include, at a minimum, the following:

''(A) Specific acquisitions, implementations, instrumentations, and operational workflows to be implemented across unclassified and classified networks, operational technology, and weapon systems.

''(B) A detailed schedule with target milestones and required expenditures.

''(C) Interim and final metrics, including a phase migration plan.

''(D) Identification of additional funding, authorities, and policies, as may be required.

''(E) Requested waivers, exceptions to Department of Defense policy, and expected delays.

''(e) IMPLEMENTATION OVERSIGHT.—

''(1) IN GENERAL.—The Chief Information Officer of the Department of Defense shall—

''(A) assess the implementation plans transmitted pursuant to subsection (d)(1) for—

''(i) adequacy and responsiveness to the zero trust strategy, principles, and model architecture required under subsection (a); and

''(ii) appropriate use of enterprise-wide acquisitions;

''(B) ensure, at a high level, the interoperability and compatibility of individual components' Solutions Architectures, including the leveraging of enterprise capabilities where appropriate through standards derivation, policy, and reviews;

''(C) use the annual investment guidance of the Chief to ensure appropriate implementation of such plans, including appropriate use of enterprise-wide acquisitions;

''(D) track use of waivers and exceptions to policy;

''(E) use the Cybersecurity Scorecard to track and drive implementation of Department components; and

''(F) leverage the authorities of the Commander of Joint Forces Headquarters-Department of Defense Information Network and the Director of the Defense Information Systems Agency to begin implementation of such zero trust strategy, principles, and model architecture.

''(2) ASSESSMENTS OF FUNDING.—Not later than March 31, 2024, and annually thereafter, each Principal Cyber Advisor of a military service shall include in the annual budget certification of such military service, as required by section 392a(c)(4) of title 10, United States Code, an assessment of the adequacy of funding requested for each proposed budget for the purposes of carrying out the implementation plan for such military service under subsection (d)(1).

''(f) INITIAL BRIEFINGS.—

''(1) ON MODEL ARCHITECTURE.—Not later than 90 days after finalizing the zero trust strategy, principles, and model architecture required under subsection (a), the Chief Information Officer of the Department of Defense and the Commander of Joint Forces Headquarters-Department of Defense Information Network shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on such zero trust strategy, principles, and model architecture.

''(2) ON IMPLEMENTATION PLANS.—Not later than 90 days after the receipt by the Chief Information Officer of the Department of Defense of an implementation plan transmitted pursuant to subsection (d)(1), the secretary of a military department, in the case of an implementation plan pertaining to a military department or a military service, or the Chief Information Officer of the Department, in the case of an implementation plan pertaining to a remaining component of the Department, as the case may be, shall provide to the congressional defense committees a briefing on such implementation plan.

''(g) ANNUAL BRIEFINGS.—Effective February 1, 2022, at each of the annual cybersecurity budget review briefings of the Chief Information Officer of the Department of Defense and the military services for congressional staff, until January 1, 2030, the Chief Information Officer and the head of each of the military services shall provide updates on the implementation in their respective networks of the zero trust strategy, principles, and model architecture.''

DEMONSTRATION PROGRAM FOR AUTOMATED SECURITY VALIDATION TOOLS

Pub. L. 117–81, div. A, title XV, §1529, Dec. 27, 2021, 135 Stat. 2048, provided that:

''(a) DEMONSTRATION PROGRAM REQUIRED.—Not later than October 1, 2024, the Chief Information Officer of the Department of Defense, acting through the Director of the Defense Information Systems Agency of the Department, shall complete a demonstration program to demonstrate and assess an automated security validation capability to assist the Department by—

''(1) mitigating cyber hygiene challenges;

''(2) supporting ongoing efforts of the Department to assess weapon systems resiliency;

''(3) quantifying enterprise security effectiveness of enterprise security controls, to inform future acquisition decisions of the Department;

''(4) assisting portfolio managers with balancing capability costs and capability coverage of the threat landscape; and

''(5) supporting the Department's Cybersecurity Analysis and Review threat framework.

''(b) CONSIDERATIONS.—In developing capabilities for the demonstration program required under subsection (a), the Chief Information Officer shall consider—

''(1) integration into automated security validation tools of advanced commercially available threat intelligence;

''(2) metrics and scoring of security controls;

''(3) cyber analysis, cyber campaign tracking, and cybersecurity information sharing;

''(4) integration into cybersecurity enclaves and existing cybersecurity controls of security instrumentation and testing capability;

''(5) endpoint sandboxing; and

''(6) use of actual adversary attack methodologies.

''(c) COORDINATION WITH MILITARY SERVICES.—In carrying out the demonstration program required under subsection (a), the Chief Information Officer, acting through the Director of the Defense Information Systems Agency, shall coordinate demonstration program activities with complementary efforts on-going within the military services, defense agencies, and field agencies.

''(d) INDEPENDENT CAPABILITY ASSESSMENT.—In carrying out the demonstration program required under subsection (a), the Chief Information Officer, acting through the Director of the Defense Information Systems Agency and in coordination with the Director, Operational Test and Evaluation, shall perform operational testing to evaluate the operational effectiveness, suitability, and cybersecurity of the capabilities developed under the demonstration program.

''(e) BRIEFING.—

''(1) INITIAL BRIEFING.—Not later than April 1, 2022, the Chief Information Officer shall brief the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives on the plans and status of the Chief Information Officer with respect to the demonstration program required under subsection (a).

''(2) FINAL BRIEFING.—Not later than October 31, 2024, the Chief Information Officer shall brief the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives on the results and findings of the Chief Information Officer with respect to the demonstration program required under subsection (a).''

CONSIDERATIONS RELATING TO PERMANENTLY BASING UNITED STATES EQUIPMENT OR ADDITIONAL FORCES IN HOST COUNTRIES WITH AT-RISK VENDORS IN 5G OR 6G NETWORKS

Pub. L. 116–283, div. A, title X, §1058, Jan. 1, 2021, 134 Stat. 3856, provided that:

''(a) IN GENERAL.—Prior to basing a major weapon system or additional permanently assigned forces comparable to or larger than a battalion, squadron, or naval combatant in a host country with at-risk 5th generation (in this section referred to as '5G') or sixth generation (in this section referred to as '6G') wireless network equipment, software, or services, including supply chain vulnerabilities identified by the Federal Acquisition Security Council, where United States military personnel and their families will be directly connected or subscribers to networks that include such at-risk equipment, software, and services in their official duties or in the conduct of personal affairs, the Secretary of Defense shall take into consideration the risks to personnel, equipment, and operations of the Department of Defense in the host country posed by current or intended use by such country of 5G or 6G telecommunications architecture provided by at-risk vendors, including Huawei and ZTE, and any steps to mitigate those risks, including—

''(1) any steps being taken by the host country to mitigate any potential risks to the weapon systems, military units, or personnel, and the Department of Defense's assessment of those efforts;

''(2) any steps being taken by the United States Government, separately or in collaboration with the host country, to mitigate any potential risks to the weapon systems, permanently deployed forces, or personnel;

''(3) any defense mutual agreements between the host country and the United States intended to allay the costs of risk mitigation posed by the at-risk infrastructure; and

''(4) any other matters the Secretary determines to be relevant.

''(b) APPLICABILITY.—The requirements under subsection (a)—

''(1) apply with respect to the permanent long-term stationing of equipment and permanently assigned forces; and

''(2) do not apply with respect to the short-term deployment or rotational presence of equipment or forces to a military installation outside the United States in connection with any exercise, dynamic force employment, contingency operation, or combat operation.

''(c) REPORT.—

''(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act [Jan. 1, 2021], 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 that contains an assessment of—

''(A) the risk to personnel, equipment, and operations of the Department of Defense in host countries posed by the current or intended use by such countries of 5G or 6G telecommunications architecture provided by at-risk vendors, including Huawei and ZTE; and

''(B) measures required to mitigate the risk described in paragraph (1).

''(2) FORM.—The report required by paragraph (1) shall be submitted in a classified form with an unclassified summary.

''(d) MAJOR WEAPON SYSTEM DEFINED.—In this section, the term 'major weapon system' has the meaning given that term in section 2379(f) of title 10, United States Code [now 10 U.S.C. 3455(f)].''

RESPONSIBILITY FOR CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION OF THE DEFENSE INDUSTRIAL BASE

Pub. L. 116–283, div. A, title XVII, §1724, Jan. 1, 2021, 134 Stat. 4111, as amended by Pub. L. 118–31, div. A, title XV, §1511, Dec. 22, 2023, 137 Stat. 541, provided that:

''(a) CRITICAL INFRASTRUCTURE DEFINED.—In this section, the term 'critical infrastructure' has the meaning given such term in section 1016(e) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (42 U.S.C. 5195c(e)).

''(b) DESIGNATION.—Not later than 30 days after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2024 [Dec. 22, 2023], the Secretary of Defense shall designate a principal staff assistant from within the Office of the Secretary of Defense who shall serve as the coordinating authority for cybersecurity issues relating to the defense industrial base.

''(c) RESPONSIBILITIES.—As the coordinating authority for cybersecurity issues relating to the defense industrial base, the principal staff assistant designated under subsection (b) shall synchronize, harmonize, deconflict, and coordinate all policies and programs germane to defense industrial base cybersecurity, including the following:

''(1) The Sector Risk Management Agency functions under Presidential Policy Directive-21 the Department of Defense has assigned to the Under Secretary of Defense for Policy for implementation.

''(2) The Under Secretary of Defense for Acquisition and Sustainment's policies and programs germane to contracting and contractual enforcement as such relate to cybersecurity assessment and assistance, and industrial base health and security.

''(3) The Under Secretary of Defense for Intelligence and Security's policies and programs germane to physical security, information security, industrial security, acquisition security and cybersecurity, all source intelligence, classified threat intelligence sharing related to defense industrial base cybersecurity activities, counterintelligence, and foreign ownership control or influence, including the Defense Intelligence Agency and National Security Agency support provided to the Department of Defense – Defense Industrial Base Collaborative Information Sharing Environment and cyber intrusion damage assessment analysis as part of defense industrial base cybersecurity activities.

''(4) The Department of Defense Chief Information Officer's policies and programs for cybersecurity standards and integrating cybersecurity threat intelligence-sharing activities and enhancing Department of Defense and defense industrial base cyber situational awareness.

''(5) The Under Secretary of Defense for Research and Engineering's policies and programs germane to protection planning requirements of emerging technologies as such relate to cybersecurity assessment and assistance, and industrial base health and security.

''(6) Other Department of Defense components' policies and programs germane to the cybersecurity of the defense industrial base, including the policies and programs of the military services and the combatant commands.

''(d) ADDITIONAL FUNCTIONS.—In carrying out this section, the principal staff assistant designated under subsection (b) shall—

''(1) coordinate or facilitate coordination with relevant Federal departments and agencies, defense industrial base entities, independent regulatory agencies, and with State, local, territorial, and Tribal entities, as appropriate;

''(2) facilitate or coordinate the provision of incident management support to defense industrial base entities, as appropriate;

''(3) facilitate or coordinate the provision of technical assistance to and consultations with defense industrial base entities to identify cyber or cyber-physical vulnerabilities and minimize the damage of potential incidents, as appropriate; and

''(4) support or facilitate the supporting of the statutorily required reporting requirements of such relevant Federal departments and agencies by providing or facilitating the provision to such departments and agencies on an annual basis relevant critical infrastructure information, as appropriate.

''(e) DEPARTMENT OF DEFENSE ROLES AND RESPONSIBILITIES.—No later than 180 days after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2024 [Dec. 22, 2023], the Secretary of Defense shall brief the Committees on Armed Services of the Senate and the House of Representatives on the following issues:

''(1) A plan for implementation of this section, including an assessment of the roles and responsibilities of entities across the Department of Defense and mechanisms and processes for coordination of policy and programs germane to defense industrial base cybersecurity.

''(2) An analysis of the feasibility and advisability of separating cybersecurity functions of a Sector Risk Management Agency pursuant to section 9002 of the National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a) from non-cybersecurity functions of a Sector Risk Management Agency.''

IMPROVING THE TRAINING WITH INDUSTRY PROGRAM

Pub. L. 116–283, div. A, title XVII, §1726(b), Jan. 1, 2021, 134 Stat. 4116, provided that:

''(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act [Jan. 1, 2021], the Principal Cyber Advisor of the Department of Defense, in consultation with the Principal Cyber Advisors of the military services and the Under Secretary of Defense for Personnel and Readiness, shall submit to the Secretary of Defense and the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a review of the current utilization and utility of the Training With Industry (TWI) programs, including relating to the following:

''(A) Recommendations regarding how to improve and better utilize such programs, including regarding individuals who have completed such programs.

''(B) An implementation plan to carry out such recommendations.

''(2) ADDITIONAL.—Not later than 90 days after the submission of the report required under paragraph (1), the Secretary of Defense shall carry out such elements of the implementation plan required under paragraph (1)(B) as the Secretary considers appropriate and notify the congressional defense committees of the determinations of the Secretary relating thereto.''

REPORTING REQUIREMENTS FOR CROSS DOMAIN INCIDENTS AND EXEMPTIONS TO POLICIES FOR INFORMATION TECHNOLOGY

Pub. L. 116–283, div. A, title XVII, §1727, Jan. 1, 2021, 134 Stat. 4117, as amended by Pub. L. 118–159, div. A, title XV, §1511, Dec. 23, 2024, 138 Stat. 2136, provided that:

''(a) INCIDENT REPORTING.—

''(1) IN GENERAL.—Effective beginning on the date of the enactment of this Act [Jan. 1, 2021], the Secretary of Defense and the secretaries of the military services shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a monthly report in writing that documents each instance or indication of a cross-domain incident within the Department of Defense.

''(2) PROCEDURES.—The Secretary of Defense shall submit to the congressional defense committees procedures for complying with the requirements of paragraph (1) consistent with the national security of the United States and the protection of operational integrity. The Secretary shall promptly notify such committees in writing of any changes to such procedures at least 14 days prior to the adoption of any such changes.

''(3) DEFINITION.—In this subsection, the term 'cross domain incident' means any unauthorized connection of any duration between software, hardware, or both that is either used on, or designed for use on a network or system built for classified data, and systems not accredited or authorized at the same or higher classification level, including systems on the public internet, regardless of whether the unauthorized connection is later determined to have resulted in the exfiltration, exposure, or spillage of data across the cross domain connection.

''(b) EXEMPTIONS TO POLICY FOR INFORMATION TECHNOLOGY.—Not later than six months after the date of the enactment of this Act and biannually thereafter, the Secretary of Defense and the secretaries of the military services shall submit to the congressional defense committees a report in writing that enumerates and details each current exemption to information technology policy, interim Authority To Operate (ATO) order, or both. Each such report shall include other relevant information pertaining to each such exemption, including relating to the following:

''(1) Risk categorization.

''(2) Duration.

''(3) Estimated time remaining.

''(c) TERMINATION DATE.—The requirement of the Secretary of Defense to submit a monthly report under subsection (a) shall terminate on December 31, 2025.''

PILOT PROGRAM ON CYBERSECURITY CAPABILITY METRICS

Pub. L. 116–283, div. A, title XVII, §1733, Jan. 1, 2021, 134 Stat. 4123, provided that:

''(a) PILOT PROGRAM REQUIRED.—The Secretary of Defense, acting through the Chief Information Officer of the Department of Defense and the Commander of United States Cyber Command, shall conduct a pilot program to assess the feasibility and advisability of developing and using speed-based metrics to measure the performance and effectiveness of security operations centers and cyber security service providers in the Department of Defense.

''(b) REQUIREMENTS.—

''(1) DEVELOPMENT OF METRICS.—(A) Not later than July 1, 2021, the Chief Information Officer and the Commander shall jointly develop metrics described in subsection (a) to carry out the pilot program under such subsection.

''(B) The Chief Information Officer and the Commander shall ensure that the metrics developed under subparagraph (A) are commensurate with the representative timelines of nation-state and non-nation-state actors when gaining access to, and compromising, Department networks.

''(2) USE OF METRICS.—(A) Not later than December 1, 2021, the Secretary shall, in carrying out the pilot program required by subsection (a), begin using the metrics developed under paragraph (1) of this subsection to assess select security operations centers and cyber security service providers, which the Secretary shall select specifically for purposes of the pilot program, for a period of not less than four months.

''(B) In carrying out the pilot program under subsection (a), the Secretary shall evaluate the effectiveness of operators, capabilities available to operators, and operators' tactics, techniques, and procedures.

''(c) AUTHORITIES.—In carrying out the pilot program under subsection (a), the Secretary may—

''(1) assess select security operations centers and cyber security service providers—

''(A) over the course of their mission performance; or

''(B) in the testing and accreditation of cybersecurity products and services on test networks designated pursuant to section 1658 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92) [set out as a note below]; and

''(2) assess select elements' use of security orchestration and response technologies, modern endpoint security technologies, Big Data Platform instantiations, and technologies relevant to zero trust architectures.

''(d) BRIEFING.—

''(1) IN GENERAL.—Not later than March 1, 2022, the Secretary shall brief the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives on the findings of the Secretary with respect to the pilot program required by subsection (a).

''(2) ELEMENTS.—The briefing provided under paragraph (1) shall include the following:

''(A) The pilot metrics developed under subsection (b)(1).

''(B) The findings of the Secretary with respect to the assessments carried out under subsection (b)(2).

''(C) An analysis of the utility of speed-based metrics in assessing security operations centers and cyber security service providers.

''(D) An analysis of the utility of the extension of the pilot metrics to or speed-based assessment of the Cyber Mission Forces.

''(E) An assessment of the technical and procedural measures that would be necessary to meet the speed-based metrics developed and applied in the pilot program.''

INTEGRATION OF DEPARTMENT OF DEFENSE USER ACTIVITY MONITORING AND CYBERSECURITY

Pub. L. 116–283, div. A, title XVII, §1735, Jan. 1, 2021, 134 Stat. 4125, provided that:

''(a) INTEGRATION OF PLANS, CAPABILITIES, AND SYSTEMS.—The Secretary of Defense shall integrate the plans, capabilities, and systems for user activity monitoring, and the plans, capabilities, and systems for endpoint cybersecurity and the collection of metadata on network activity for cybersecurity to enable mutual support and information sharing.

''(b) REQUIREMENTS.—In carrying out subsection (a), the Secretary shall—

''(1) consider using the Big Data Platform instances that host cybersecurity metadata for storage and analysis of all user activity monitoring data collected across the Department of Defense Information Network at all security classification levels;

''(2) develop policies and procedures governing access to user activity monitoring data or data derived from user activity monitoring by cybersecurity operators; and

''(3) develop processes and capabilities for using metadata on host and network activity for user activity monitoring in support of the insider threat mission.

''(c) CONGRESSIONAL BRIEFING.—Not later than October 1, 2021, the Secretary shall provide a briefing to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] on actions taken to carry out this section.''

ASSESSMENT ON DEFENSE INDUSTRIAL BASE PARTICIPATION IN A THREAT INFORMATION SHARING PROGRAM

Pub. L. 116–283, div. A, title XVII, §1737, Jan. 1, 2021, 134 Stat. 4127, provided that:

''(a) DEFENSE INDUSTRIAL BASE THREAT INFORMATION PROGRAM ASSESSMENT.—Not later than 270 days after the date of the enactment of this Act [Jan. 1, 2021], the Secretary of Defense shall complete an assessment of the feasibility, suitability, and definition of, and resourcing required to establish, a defense industrial base threat information sharing program to collaborate and share threat information with, and obtain threat information from, the defense industrial base.

''(b) ELEMENTS.—The assessment regarding the establishment of a defense industrial base threat information sharing program under subsection (a) shall include evaluation of the following:

''(1) The feasibility and suitability of, and requirements for, the establishment of a defense industrial base threat information sharing program, including cybersecurity incident reporting requirements applicable to the defense industrial base that—

''(A) extend beyond mandatory cybersecurity incident reporting requirements as in effect on the day before the date of the enactment of this Act;

''(B) set specific, consistent timeframes for all categories of cybersecurity incident reporting;

''(C) establish a single clearinghouse for all mandatory cybersecurity incident reporting to the Department of Defense, including incidents involving covered unclassified information, and classified information; and

''(D) provide that, unless authorized or required by another provision of law or the element of the defense industrial base making the report consents, nonpublic information of which the Department becomes aware only because of a report provided pursuant to the program shall be disseminated and used only for a cybersecurity purpose (as such term is defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501)) and in support of national defense activities.

''(2) A mechanism for developing a shared and real-time picture of the threat environment.

''(3) Options for joint, collaborative, and co-located analytics.

''(4) Possible investments in technology and capabilities to support automated detection and analysis across the defense industrial base.

''(5) Coordinated information tipping, sharing, and deconfliction, as necessary, with relevant Federal Government agencies with similar information sharing programs.

''(6) Processes for direct sharing of threat information related to a specific defense industrial base entity with such entity.

''(7) Mechanisms for providing defense industrial base entities with clearances for national security information access, as appropriate.

''(8) Requirements to consent to queries of foreign intelligence collection databases related to a specific defense industrial base entity as a condition of participation in the threat information sharing program.

''(9) Recommendations with respect to threat information sharing program participation, including the following:

''(A) Incentives for defense industrial base entities to participate in the threat information sharing program.

''(B) Mandating minimum levels of threat information sharing program participation for any entity that is part of the defense industrial base.

''(C) Procurement prohibitions on any defense industrial base entity that are not in compliance with the requirements of the threat information sharing program.

''(D) Waiver authority and criteria.

''(E) Adopting tiers of requirements for participation within the threat information sharing program based on—

''(i) the role of and relative threats related to defense industrial base entities; and

''(ii) Cybersecurity Maturity Model Certification level.

''(10) Options to utilize an existing federally recognized information sharing program to satisfy the re-

quirement for a threat information sharing program if—

''(A) the existing program includes, or is modified to include, two-way sharing of threat information that is specifically relevant to the defense industrial base; and

''(B) such a program is coordinated with other Federal Government agencies with existing information sharing programs where overlap occurs.

''(11) Methods to encourage participation of defense industrial base entities in appropriate private sector information sharing and analysis centers (ISACs).

''(12) Methods to coordinate collectively with defense industrial base entities to consider methods for mitigating compliance costs.

''(13) The resources needed, governance roles and structures required, and changes in regulation or law needed for execution of a threat information sharing program, as well as any other considerations determined relevant by the Secretary.

''(14) Identification of any barriers that would prevent the establishment of a defense industrial base threat information sharing program.

''(c) CONSULTATION.—In conducting the assessment required under subsection (a), the Secretary of Defense shall consult with and solicit recommendations from representative industry stakeholders across the defense industrial base regarding the elements described in subsection (b) and potential stakeholder costs of compliance.

''(d) DETERMINATION AND BRIEFING.—Upon completion of the assessment required under subsection (a), the Secretary of Defense shall make a determination regarding the establishment by the end of fiscal year 2021 of a defense industrial base threat information sharing program and provide a briefing to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives on—

''(1) the findings of the Secretary with respect to such assessment and such determination; and

''(2) such implementation plans as the Secretary may have arising from such findings.

''(e) IMPLEMENTATION.—If the Secretary of Defense makes a positive determination pursuant to subsection (d) of the feasibility and suitability of establishing a defense industrial base threat information sharing program, the Secretary shall establish such program. Not later than 180 days after a positive determination, the Secretary of Defense shall promulgate such rules and regulations as are necessary to establish the defense industrial base threat information sharing program under this section.''

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

Pub. L. 116–283, div. A, title XVII, §1738, Jan. 1, 2021, 134 Stat. 4129, provided that:

''(a) IN GENERAL.—Subject to the availability of appropriations, the Secretary of Defense, in consultation with the Director of the National Institute of Standards and Technology, may award financial assistance to a Center for the purpose of providing cybersecurity services to small manufacturers.

''(b) CRITERIA.—If the Secretary carries out subsection (a), the Secretary, in consultation with the Director, shall establish and publish on the grants.gov website, or successor website, criteria for selecting recipients for financial assistance under this section.

''(c) USE OF FINANCIAL ASSISTANCE.—Financial assistance under this section—

''(1) shall be used by a Center to provide small manufacturers with cybersecurity services, including—

''(A) compliance with the cybersecurity requirements of the Department of Defense Supplement to the Federal Acquisition Regulation, including awareness, assessment, evaluation, preparation, and implementation of cybersecurity services; and

''(B) achieving compliance with the Cybersecurity Maturity Model Certification framework of the Department of Defense; and

''(2) may be used by a Center to employ trained personnel to deliver cybersecurity services to small manufacturers.

''(d) BIENNIAL REPORTS.—

''(1) IN GENERAL.—Not less frequently than once every two years, the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives], the Committee on Commerce, Science, and Transportation of the Senate, and the Committee on Science, Space, and Technology of the House of Representatives a report on financial assistance awarded under this section.

''(2) CONTENTS.—To the extent practicable, each report submitted under paragraph (1) shall include the following with respect to the years covered by each such report:

''(A) The number of small manufacturers assisted.

''(B) A description of the cybersecurity services provided.

''(C) A description of the cybersecurity matters addressed.

''(D) An analysis of the operational effectiveness and cost-effectiveness of such cybersecurity services.

''(e) TERMINATION.—The authority of the Secretary to award financial assistance under this section shall terminate on the date that is five years after the date of the enactment of this section [Jan. 1, 2021].

''(f) DEFINITIONS.—In this section:

''(1) CENTER.—The term 'Center' has the meaning given such term in section 25(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278k(a)).

''(2) SMALL MANUFACTURER.—The term 'small manufacturer' has the meaning given such term in section 1644(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. 2224 note).''

ASSESSMENT ON DEFENSE INDUSTRIAL BASE CYBERSECURITY THREAT HUNTING PROGRAM

Pub. L. 116–283, div. A, title XVII, §1739, Jan. 1, 2021, 134 Stat. 4130, provided that:

''(a) ASSESSMENT REQUIRED.—Not later than 270 days after the date of the enactment of this Act [Jan. 1, 2021], the Secretary of Defense shall complete an assessment of the feasibility, suitability, definition of, and resourcing required to establish a defense industrial base cybersecurity threat hunting program to actively identify cybersecurity threats and vulnerabilities within the defense industrial base.

''(b) ELEMENTS.—The assessment required under section [sic] (a) shall include evaluation of the following:

''(1) Existing defense industrial base cybersecurity threat hunting policies and programs, including the threat hunting elements at each level of the compliance-based Cybersecurity Maturity Model Certification program of the Department of Defense, including requirements germane to continuous monitoring, discovery, and investigation of anomalous activity indicative of a cybersecurity incident.

''(2) The suitability of a continuous cybersecurity threat hunting program, as a supplement to the cyber hygiene requirements of the Cybersecurity Maturity Model Certification, including consideration of the following:

''(A) Collection and analysis of metadata on network activity to detect possible intrusions.

''(B) Rapid investigation and remediation of possible intrusions.

''(C) Requirements for mitigating any vulnerabilities identified pursuant to the cybersecurity threat hunting program.

''(D) Mechanisms for the Department of Defense to share with entities in the defense industrial base malicious code, indicators of compromise, and insights on the evolving threat landscape.

''(3) Recommendations with respect to cybersecurity threat hunting program participation

of prime contractors and subcontractors, including relating to the following:

''(A) Incentives for defense industrial base entities to share with the Department of Defense threat and vulnerability information collected pursuant to threat monitoring and hunting activities.

''(B) Mandating minimum levels of program participation for any defense industrial base entity.

''(C) Procurement prohibitions on any defense industrial base entity that is not in compliance with the requirements of the cybersecurity threat hunting program.

''(D) Waiver authority and criteria.

''(E) Consideration of a tiered cybersecurity threat hunting program that takes into account the following:

''(i) The cybersecurity maturity of defense industrial base entities.

''(ii) The roles of such entities.

''(iii) Whether each such entity possesses classified information or controlled unclassified information and covered defense networks.

''(iv) The covered defense information to which each such entity has access as a result of contracts with the Department of Defense.

''(4) Whether the continuous cybersecurity threat-hunting program described in paragraph (2) should be conducted by—

''(A) qualified prime contractors or subcontractors;

''(B) accredited third-party cybersecurity vendors;

''(C) with contractor consent—

''(i) United States Cyber Command; or

''(ii) a component of the Department of Defense other than United States Cyber Command;

''(D) the deployment of network sensing technologies capable of identifying and filtering malicious network traffic; or

''(E) a combination of the entities specified in subparagraphs (A) through (D).

''(5) The resources necessary, governance structures or changes in regulation or law needed, and responsibility for execution of a defense industrial base cybersecurity threat hunting program, as well as any other considerations determined relevant by the Secretary.

''(6) A timelime [sic] for establishing the defense industrial base cybersecurity threat hunting program not later than two years after the date of the enactment of this Act [Jan. 1, 2021].

''(7) Identification of any barriers that would prevent such establishment.

''(c) CONSULTATION.—In conducting the assessment required under subsection (a), the Secretary of Defense shall consult with and solicit recommendations from representative industry stakeholders across the defense industrial base regarding the elements described in subsection (b) and potential stakeholder costs of compliance.

''(d) DETERMINATION AND BRIEFING.—Upon completion of the assessment required under subsection (a), the Secretary of Defense shall make a determination regarding the establishment of a defense industrial base cybersecurity threat hunting program and provide a briefing to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives on—

''(1) the findings of the Secretary with respect to such assessment and such determination; and

''(2) such implementation plans as the Secretary may have arising from such findings.

''(e) IMPLEMENTATION.—If the Secretary of Defense makes a positive determination pursuant to subsection (d) of the feasibility and suitability of establishing a defense industrial base threat cybersecurity threat hunting program, the Secretary shall establish such program. Not later than 180 days after a positive determination, the Secretary of Defense shall promulgate such rules and regulations as are necessary to establish the defense industrial base cybersecurity threat hunting program under this section.''

ROLE OF CHIEF INFORMATION OFFICER IN IMPROVING ENTERPRISE-WIDE CYBERSECURITY

Pub. L. 116–92, div. A, title XVI, §1641, Dec. 20, 2019, 133 Stat. 1750, provided that:

''(a) IN GENERAL.—In carrying out the responsibilities established in section 142 of title 10, United States Code, the Chief Information Officer of the Department of Defense shall, to the maximum extent practicable, ensure that the cybersecurity programs and capabilities of the Department—

''(1) fit into an enterprise-wide cybersecurity architecture;

''(2) are maximally interoperable with each other, including those programs and capabilities deployed by the components of the Department;

''(3) enhance enterprise-level visibility and responsiveness to threats; and

''(4) are developed, procured, instituted, and managed in a cost-efficient manner, exploiting economies of scale and enterprise-wide services and discouraging unnecessary customization and piecemeal acquisition.

''(b) REQUIREMENTS.—In carrying out subsection (a), the Chief Information Officer shall—

''(1) manage and modernize the cybersecurity architecture of the Department, including—

''(A) ensuring the cybersecurity architecture of the Department maximizes cybersecurity capability, network, and endpoint activity data sharing across Department components;

''(B) ensuring the cybersecurity architecture of the Department supports improved automaticity of cybersecurity detection and response; and

''(C) modernizing and configuring the Department's standardized deployed perimeter, network-level, and endpoint capabilities to improve interoperability, meet pressing capability needs, and negate common adversary tactics, techniques, and procedures;

''(2) establish mechanisms to enable and mandate, as necessary, cybersecurity capability and network and endpoint activity data-sharing across Department components;

''(3) make mission data, through data tagging, automatic transmission, and other means, accessible and discoverable by Department components other than owners of such mission data;

''(4) incorporate into the cybersecurity architecture of the Department emerging cybersecurity technologies from the Defense Advanced Research Projects Agency, the Strategic Capabilities Office, the Defense Innovation Unit, the laboratories of the military departments, and the commercial sector;

''(5) ensure that the Department possesses the necessary computing infrastructure, through technology refresh, installation or acquisition of bandwidth, and the use of cloud computing power, to host and enable necessary cybersecurity capabilities; and

''(6) utilize the Department's cybersecurity expertise to improve cybersecurity performance, operations, and acquisition, including—

''(A) the cybersecurity testing, architecting, and engineering expertise of the National Security Agency; and

''(B) the technology policy, workforce, and engineering expertise of the Defense Digital Service.''

CONTROL AND ANALYSIS OF DEPARTMENT OF DEFENSE DATA STOLEN THROUGH CYBERSPACE

Pub. L. 116–92, div. A, title XVI, §1646, Dec. 20, 2019, 133 Stat. 1753, provided that:

''(a) REQUIREMENTS.—If the Secretary of Defense determines that significant Department of Defense data may have been stolen through cyberspace and evidence of theft of the data in question—

''(1) is in the possession of a component of the Department, the Secretary shall—

''(A) either transfer or replicate and transfer such Department data in a prompt and secure manner to a secure repository with access by Department personnel appropriately limited on a need-to-know basis or otherwise ensure such consistent access to the relevant data by other means;

''(B) ensure the Department applies such automated analytic tools and capabilities to the repository of potentially compromised data as are necessary to rapidly understand the scope and effect of the potential compromise;

''(C) for high priority and mission critical Department systems, develop analytic products that characterize the scope of data compromised;

''(D) ensure that relevant mission-affected entities in the Department are made aware of the theft or possible theft and, as damage assessment and mitigation proceeds, are kept apprised of the extent of the data stolen; and

''(E) ensure that Department counterintelligence organizations are—

''(i) fully integrated with any damage assessment team assigned to the breach;

''(ii) fully informed of the data that have or potentially have been stolen and the effect of such theft; and

''(iii) provided resources and tasked, in conjunction with subject matter experts and responsible authorities, to immediately and appropriately respond, including through the development and execution of relevant countermeasures, to any breach involving espionage and data theft; or

''(2) is in the possession of or under controls or restrictions imposed by the Federal Bureau of Investigation, or a national counterintelligence or intelligence organization, the Secretary shall determine, jointly with the Director of the Federal Bureau of Investigation or the Director of National Intelligence, as appropriate, the most expeditious process, means, and conditions for carrying out the activities otherwise required by paragraph (1).

''(b) RECOMMENDATIONS.—Not later than 90 days after the date of the enactment of this Act [Dec. 20, 2019], the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] such recommendations as the Secretary may have for legislative or administrative action to address such barriers that may be inhibiting the implementation of this section.''

USE OF NATIONAL SECURITY AGENCY CYBERSECURITY EXPERTISE TO SUPPORT EVALUATION OF COMMERCIAL CYBERSECURITY PRODUCTS

Pub. L. 116–92, div. A, title XVI, §1647, Dec. 20, 2019, 133 Stat. 1754, as amended by Pub. L. 116–283, div. A, title X, §1081(c)(7), Jan. 1, 2021, 134 Stat. 3873, provided that:

''(a) ADVISORY MISSION.—The National Security Agency shall, as a mission in its role in securing the information systems of the Department of Defense, advise and assist the Department of Defense in its evaluation and adoption of cybersecurity products and services from industry, especially the commercial cybersecurity sector.

''(b) PROGRAM TO IMPROVE ACQUISITION OF CYBERSECURITY PRODUCTS AND SERVICES.—

''(1) ESTABLISHMENT.—Consistent with subsection (a), the Director of the National Security Agency shall establish a permanent program consisting of market research, testing, and expertise transmission, or augments to existing programs, to improve the evaluation by the Department of Defense of cybersecurity products and services.

''(2) REQUIREMENTS.—Under the program established pursuant to paragraph (1), the Director shall, independently and at the request of the components of the Department of Defense—

''(A) test and evaluate commercially available cybersecurity products and services using—

''(i) generally known cyber operations techniques; and

''(ii) tools and cyber operations techniques and advanced tools and techniques available to the National Security Agency;

''(B) develop and establish standard procedures, techniques, and threat-informed metrics to perform the testing and evaluation required by subparagraph (A); and

''(C) advise the Chief Information Officer and the components of the Department of Defense on the merits and disadvantages of evaluated cybersecurity products, including with respect to—

''(i) any synergies between products;

''(ii) value;

''(iii) matters relating to operation and maintenance; and

''(iv) matters relating to customization requirements.

''(3) LIMITATIONS.—The program established under paragraph (1) may not—

''(A) be used to accredit cybersecurity products and services for use by the Department;

''(B) create approved products lists; or

''(C) be used for the procurement and fielding of cybersecurity products on behalf of the Department.''

[Pub. L. 116–283, div. A, title X, §1081(c), Jan. 1, 2021, 134 Stat. 3873, provided that the amendment made by section 1081(c)(7) of Pub. L. 116–283 to section 1647 of Pub. L. 116–92, set out above, is effective as of Dec. 20, 2020 (probably should be Dec. 20, 2019) and as if included in Pub. L. 116–92.]

FRAMEWORK TO ENHANCE CYBERSECURITY OF THE UNITED STATES DEFENSE INDUSTRIAL BASE

Pub. L. 116–92, div. A, title XVI, §1648, Dec. 20, 2019, 133 Stat. 1755, as amended by Pub. L. 117–81, div. A, title XV, §1526, Dec. 27, 2021, 135 Stat. 2043, provided that:

''(a) FRAMEWORK REQUIRED.—Not later than 180 days after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2022 [Dec. 27, 2021], the Secretary of Defense shall develop a consistent, comprehensive framework to enhance cybersecurity for the United States defense industrial base.

''(b) ELEMENTS.—The framework developed pursuant to subsection (a) shall include the following:

''(1) Identification of unified cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements to be imposed on the defense industrial base for the purpose of assessing the cybersecurity of individual contractors.

''(2) Roles and responsibilities of the Under Secretary of Defense for Acquisition and Sustainment, the Under Secretary of Defense for Intelligence and Security, the Chief Information Officer, the Director of the Protecting Critical Technologies Task Force, and the Secretaries of the military departments relating to the following:

''(A) Establishing and ensuring compliance with cybersecurity standards, regulations, and policies.

''(B) Deconflicting existing cybersecurity standards, regulations, and policies.

''(C) Coordinating with and providing assistance to the defense industrial base for cybersecurity matters, particularly as relates to the programs and processes described in paragraphs (8) and (9).

''(D) Management and oversight of the acquisition process, including responsibility determination, solicitation, award, and contractor management, relating to cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements.

''(3) The responsibilities of the prime contractors, and all subcontractors in the supply chain, for implementing the required cybersecurity standards, regulations, metrics, ratings, third-party certifications, and requirements identified under paragraph (1).

''(4) Definitions for 'Controlled Unclassified Information' (CUI) and 'For Official Use Only' (FOUO),

policies regarding protecting information designated as either of such, and an explanation of the 'DoD CUI Program' and Department of Defense compliance with the responsibilities specified in Department of Defense Instruction (DoDI) 5200.48, 'Controlled Unclassified Information (CUI),' including the following:

''(A) The extent to which the Department of Defense is identifying whether information is CUI via a contracting vehicle and marking documents, material, and media containing such information in a clear and consistent manner.

''(B) Recommended regulatory or policy changes to ensure consistency and clarity in CUI identification and marking requirements.

''(C) Circumstances under which commercial information is considered CUI, and any impacts to the commercial supply chain associated with security and marking requirements pursuant to this paragraph.

''(D) Benefits and drawbacks of requiring all CUI to be marked with a unique CUI legend, versus requiring that all data marked with an appropriate restricted legend be handled as CUI.

''(E) The extent to which the Department of Defense clearly delineates Federal Contract Information (FCI) from CUI.

''(F) Examples or scenarios to illustrate information that is and is not CUI.

''(5) Methods and programs for managing controlled unclassified information, and for limiting the presence of unnecessary sensitive information on contractor networks.

''(6) A plan to provide implementation guidance, education, manuals, and, as necessary, direct technical support or assistance, to contractors on matters relating to cybersecurity.

''(7) Quantitative metrics for assessing the effectiveness of the overall framework over time, with respect to the exfiltration of controlled unclassified information from the defense industrial base.

''(8) A comprehensive list of current and planned Department of Defense programs to assist the defense industrial base with cybersecurity compliance requirements of the Department, including those programs that provide training, expertise, and funding, and maintain approved security products lists and approved providers lists.

''(9) Processes for enhanced threat information sharing between the Department of Defense and the defense industrial base.

''(c) MATTERS FOR CONSIDERATION.—In developing the framework pursuant to subsection (a), the Secretary shall consider the following:

''(1) Designating an official to be responsible for the cybersecurity of the defense industrial base.

''(2) Risk-based methodologies, standards, metrics, and tiered cybersecurity requirements for the defense industrial base, including third-party certifications such as the Cybersecurity Maturity Model Certification pilot program, as the basis for a mandatory Department standard.

''(3) Tailoring cybersecurity requirements for small- and medium-sized contractors based on a risk-based approach.

''(4) Ensuring a consistent approach across the Department to cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements of the defense industrial base.

''(5) Ensuring the Department's traceability and visibility of cybersecurity compliance of suppliers to all levels of the supply chain.

''(6) Evaluating incentives and penalties for cybersecurity performance of suppliers.

''(7) Integrating cybersecurity and traditional counterintelligence measures, requirements, and programs.

''(8) Establishing a secure software development environment (DevSecOps) in a cloud environment inside the perimeter of the Department for contractors to perform their development work.

''(9) Establishing a secure cloud environment through which contractors may access the data of the Department needed for their contract work.

''(10) An evaluation of the resources and utilization of Department programs to assist the defense industrial base in complying with cybersecurity compliance requirements referred to in subsection (b)(1).

''(11) Technological means, operational concepts, reference architectures, offensive counterintelligence operation concepts, and plans for operationalization to complicate adversary espionage, including honeypotting and data obfuscation.

''(12) Implementing enhanced security vulnerability assessments for contractors working on critical acquisition programs, technologies, manufacturing capabilities, and research areas.

''(13) Identifying ways to better leverage technology and employ machine learning or artificial intelligence capabilities, such as Internet Protocol monitoring and data integrity capabilities, to be applied to contractor information systems that host, receive, or transmit controlled unclassified information.

''(14) Developing tools to easily segregate program data to only allow subcontractors access to their specific information.

''(15) Appropriate communications of threat assessments of the defense industrial base to the acquisition workforce at all classification levels.

''(16) A single Sector Coordinating Council for the defense industrial base.

''(17) Appropriate communications with the defense industrial base on the impact of cybersecurity requirements in contracting and procurement decisions.

''(d) CONSULTATION.—In developing the framework required pursuant to subsection (a), the Secretary shall consult with the following:

''(1) Industry groups representing the defense industrial base.

''(2) Contractors in the defense industrial base.

''(3) The Director of the National Institute of Standards and Technology.

''(4) The Secretary of Energy.

''(5) The Director of National Intelligence.

''(6) Relevant Federal regulatory agencies.

''(e) BRIEFING.—

''(1) IN GENERAL.—Not later than March 11, 2020, the Secretary of Defense shall provide the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] with a briefing on the framework developed pursuant to subsection (a).

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

''(A) An overview of the framework developed pursuant to subsection (a).

''(B) Identification of such pilot programs as the Secretary considers may be required to improve the cybersecurity of the defense industrial base.

''(C) Implementation timelines and identification of costs.

''(D) Such recommendations as the Secretary may have for legislative action to improve the cybersecurity of the defense industrial base.

''(f) QUARTERLY BRIEFINGS.—

''(1) IN GENERAL.—Not less frequently than once each quarter after the briefing provided pursuant to subsection (e) until February 1, 2022, the Secretary of Defense shall brief the congressional defense committees on the status of development and implementation of the framework developed pursuant to subsection (a).

''(2) COORDINATION WITH OTHER BRIEFINGS.—Each briefing under paragraph (1) shall be conducted in conjunction with a quarterly briefing under section 484(a) of title 10, United States Code.

''(3) ELEMENTS.—Each briefing under paragraph (1) shall include the following:

''(A) The current status of the development and implementation of the framework developed pursuant to subsection (a).

''(B) A description of the efforts undertaken by the Secretary to evaluate the matters for consideration set forth in subsection (c).

''(C) The current status of any pilot programs the Secretary is carrying out to develop the framework.''

DESIGNATION OF TEST NETWORKS FOR TESTING AND ACCREDITATION OF CYBERSECURITY PRODUCTS AND SERVICES

Pub. L. 116–92, div. A, title XVI, §1658, Dec. 20, 2019, 133 Stat. 1769, provided that:

''(a) DESIGNATION.—Not later than April 1, 2020, the Secretary of Defense shall designate, for use by the Defense Information Systems Agency and such other components of the Department of Defense as the Secretary considers appropriate, three test networks for the testing and accreditation of cybersecurity products and services.

''(b) REQUIREMENTS.—The networks designated under subsection (a) shall—

''(1) be of sufficient scale to realistically test cybersecurity products and services;

''(2) feature substantially different architectures and configurations;

''(3) be live, operational networks; and

''(4) feature cybersecurity processes, tools, and technologies that are appropriate for test purposes and representative of the processes, tools, and technologies that are widely used throughout the Department.

''(c) ACCESS.—Upon request, information generated in the testing and accreditation of cybersecurity products and services shall be made available to the Office of the Director, Operational Test and Evaluation.''

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 com-

mittees 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 National 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, as amended by Pub. L. 116–283, div. A, title XVIII, §§ 1844(e)(2), 1869(e), Jan. 1, 2021, 134 Stat. 4246, 4284; Pub. L. 117–81, div. A, title XVII, § 1701(u)(5)(B), Dec. 27, 2021, 135 Stat. 2154, 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 4841 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 [now 10 U.S.C. 4124].

''(3) The Manufacturing Engineering Education Program established under section 2196 of title 10, United States Code [now 10 U.S.C. 4843].

''(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 [now Committee on Oversight and Accountability] 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 [now Committee on Oversight and Accountability] 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, prod-

uct 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 [now Committee on Oversight and Accountability] 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, as amended by Pub. L. 116–283, div. A, title XVII, §1712(b), Jan. 1, 2021, 134 Stat. 4087; Pub. L. 117–81, div. A, title XV, §1525, Dec. 27, 2021, 135 Stat. 2043; Pub. L. 117–263, div. A, title XV, §1503, Dec. 23, 2022, 136 Stat. 2880, which provided for the establishment of the Strategic Cybersecurity Program to ensure the Department of Defense's ability to conduct the most important military missions of the Department, was repealed by Pub. L. 118–31, div. A, title XV, §1502(a)(2)(C), Dec. 22, 2023, 137 Stat. 537. See section 391b of this title.

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; Pub. L. 118–31, div. A, title XV, §1502(a)(2)(B), Dec. 22, 2023, 137 Stat. 537, 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 Representatives] 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) 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.

''(e) 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; Pub. L. 116–92, div. A, title VIII, §821, Dec. 20, 2019, 133 Stat. 1490; Pub. L. 116–283, div. A, title XVII, §1711, Jan. 1, 2021, 134 Stat. 4086, 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) 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.).

''(f) 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.

''(g) 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.''

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; Pub. L. 116–92, div. A, title XVI, §1633, Dec. 20, 2019, 133 Stat. 1746; Pub. L. 116–283, div. A, title XVII, §1712(a), Jan. 1, 2021, 134 Stat. 4087; Pub. L. 118–31, div. A, title XV, §1502(a)(2)(A), Dec. 22, 2023, 137 Stat. 537, 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 evalua-

tions 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) 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.

''(d) 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.

''(e) 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).

''(f) WRITTEN NOTIFICATION.—If the Secretary determines that the Department will not complete an evaluation of the cyber vulnerabilities of each major weapon system of the Department by the date specified in subsection (a)(1), the Secretary shall provide to the congressional defense committees written notification relating to each such incomplete evaluation. Such a written notification shall include the following:

''(1) An identification of each major weapon system for which an evaluation will not be complete by the date specified in subsection (a)(1), the anticipated date of completion of the evaluation of each such weapon system, and a description of the remaining work to be done for the evaluation of each such weapon system.

''(2) A justification for the inability to complete such an evaluation by the date specified in subsection (a)(1).

''(g) REPORT.—The Secretary, acting through the Under Secretary of Defense for Acquisition and Sustainment, shall provide a report to the congressional defense committees upon completion of the requirement for an evaluation of the cyber vulnerabilities of each major weapon system of the Department under this section. Such report shall include the following:

''(1) An identification of cyber vulnerabilities of each major weapon system requiring mitigation.

''(2) An identification of current and planned efforts to address the cyber vulnerabilities of each major weapon system requiring mitigation, including efforts across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities of the Department.

''(3) A description of joint and common cyber vulnerability mitigation solutions and efforts, including solutions and efforts across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities of the Department.

''(4) A description of lessons learned and best practices regarding evaluations of the cyber vulnerabilities and cyber vulnerability mitigation efforts relating to major weapon systems, including an identification of useful tools and technologies for discovering and mitigating vulnerabilities, such as those specified in section 1657 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232) [132 Stat. 2151], and steps taken to institutionalize the use of these tools and technologies.

''(5) A description of efforts to share lessons learned and best practices regarding evaluations of the cyber vulnerabilities and cyber vulnerability mitigation efforts of major weapon systems across the Department.

''(6) An identification of measures taken to institutionalize evaluations of cyber vulnerabilities of major weapon systems, including an identification of which major weapon systems evaluated under this section will be reevaluated in the future, when these evaluations will occur, and how evaluations will occur for future major weapon systems.

''(7) Information relating to guidance, processes, procedures, or other activities established to mitigate or address the likelihood of cyber vulnerabilities of major weapon systems by incorporation of lessons learned in the research, development, test, evaluation, and acquisition cycle, including promotion of cyber education of the acquisition workforce.

''(8) An identification of systems to be incorporated into or that have been incorporated into the National Security Agency's Strategic Cybersecurity Program and the status of these systems in the Program.

''(9) Any other matters the Secretary determines relevant.

''(h) ESTABLISHING REQUIREMENTS FOR PERIODICITY OF VULNERABILITY REVIEWS.—The Secretary of Defense shall establish policies and requirements for each major weapon system, and the priority critical infrastructure essential to the proper functioning of major weapon systems in broader mission areas, to be re-assessed for cyber vulnerabilities, taking into account upgrades or other modifications to systems and changes in the threat landscape.

''(i) IDENTIFICATION OF SENIOR OFFICIAL.—Each secretary of a military department shall identify a senior official who shall be responsible for ensuring that cyber vulnerability assessments and mitigations for weapon systems and critical infrastructure are planned, funded, and carried out.''

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, as amended by Pub. L. 116–283, div. A, title XVII, § 1713(a), Jan. 1, 2021, 134 Stat. 4089; Pub. L. 117–81, div. A, title XV, § 1503(a), Dec. 27, 2021, 135 Stat. 2021; Pub. L. 117–263, div. A, title X, § 1081(d), title XV, § 1501(a), (b)(2)(A), (B), Dec. 23, 2022, 136 Stat. 2797, 2877, 2878, 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) Transferred to section 392a(a) of this title.]

''(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, as amended by Pub. L. 117–263, div. A, title XV, § 1501(c)(3), Dec. 23, 2022, 136 Stat. 2879, provided that: ''The Principal Cyber Advisor to the Secretary of Defense, acting through the cross-functional team under section 392a(a)(3) of title 10, United States Code, 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, which provided for the establishment of a joint federation of capabilities to support the trusted defense system needs of the Department of Defense, was repealed by Pub. L. 118–159, div. A, title IX, § 922(c), Dec. 23, 2024, 138 Stat. 2039. See section 4128 of this title.

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, as amended by Pub. L. 116–283, div. A, title XVIII, § 1806(e)(2)(A), Jan. 1, 2021, 134 Stat. 4155, 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 3041 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, as amended by Pub. L. 116–283, div. A, title XVIII, §1806(e)(2)(B), Jan. 1, 2021, 134 Stat. 4155, 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 3041 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 de-

fense 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.)

Editorial Notes

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.

[1] See References in Text note below.

[§ 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.

Statutory Notes and Related Subsidiaries

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 actions covered by such section entered into on or after Oct. 30, 2000, was repealed by Pub. L. 114–328, div. A, title VIII, §833(b)(2)(C)(i), Dec. 23, 2016, 130 Stat. 2284.

GAO REPORT

Pub. L. 106–398, §1 [[div. A], title VIII, §812(c)], Oct. 30, 2000, 114 Stat. 1654, 1654A–214, which directed the Comptroller General to submit to committees of Congress a report on the collection of data under this section not later than 15 months after Oct. 30, 2000, was repealed by Pub. L. 114–328, div. A, title VIII, §833(b)(2)(C)(i), Dec. 23, 2016, 130 Stat. 2284.

[§ 2226. Renumbered § 4602]

[§ 2227. Renumbered § 4601]

§ 2228. Office of Corrosion Policy and Oversight

(a) OFFICE AND DIRECTOR.—(1) There is an Office of Corrosion Policy and Oversight within the Office of the Under Secretary of Defense for Acquisition and Sustainment.

(2) The Office shall be headed by a Director of Corrosion Policy and Oversight, who shall be assigned to such position by the Under Secretary from among civilian employees of the Department of Defense with the qualifications described in paragraph (3). The Director is responsible in the Department of Defense to the Secretary of Defense (after the Under Secretary of Defense for Acquisition and Sustainment) for the prevention and mitigation of corrosion of the military equipment and infrastructure of the Department of Defense.

(3) In order to qualify to be assigned to the position of Director, an individual shall—

(A) have management expertise in, and professional experience with, corrosion project and policy implementation, including an understanding of the effects of corrosion policies on infrastructure; research, development, test, and evaluation; and maintenance; and

(B) have an understanding of Department of Defense budget formulation and execution, policy formulation, and planning and program requirements.

(4) The Secretary of Defense shall designate the position of Director as a critical acquisition position under section 1731 of this title.