Editorial Notes

REFERENCES IN TEXT

Sections 1533 and 1534 of the National Defense Authorization Act for Fiscal Year 2023, referred to in subsec. (a)(1), are sections 1533 and 1534 of Pub. L. 117–263, also known as the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, which are set out as notes under section 167b of this title.

Statutory Notes and Related Subsidiaries

FIRST REPORT

Pub. L. 117–263, div. A, title XV, § 1502(b), Dec. 23, 2022, 136 Stat. 2880, provided that: ''The Commander of the United States Cyber Command shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] the first report under section 391a of title 10, United States Code, as added by subsection (a), as soon as practicable after the date of the submission of the defense budget materials for fiscal year 2024.''

§ 391b. Strategic cybersecurity program

(a) IN GENERAL.—(1) There is a program to be known as the ''Strategic Cybersecurity Program'' (in this section referred to as the ''Program'') to ensure the ability of the Department of Defense to conduct the most critical military missions of the Department.

(2) The Secretary of Defense shall designate a principal staff assistant from within the Office of the Secretary of Defense whose office shall serve as the office of primary responsibility for the Program, and provide policy, direction, and oversight regarding the execution of the responsibilities of the program manager selected pursuant to subsection (c)(1).

(b) MEMBERSHIP.—In addition to the office of primary responsibility for the Program under subsection (a)(2) and the program manager selected pursuant to subsection (c)(1), membership in the Program shall include the following:

(1) The Vice Chairman of the Joint Chiefs of Staff.

(2) The Commanders of the United States Cyber Command, United States European Command, United States Indo-Pacific Command, United States Northern Command, United States Strategic Command, United States Space Command, United States Transportation Command.

(3) The Under Secretary of Defense for Acquisition and Sustainment.

(4) The Under Secretary of Defense for Policy.

(5) The Chief Information Officer of the Department of Defense.

(6) The Chief Digital and Artificial Intelligence Officer of the Department of Defense.

(7) The chief information officers of the military departments.

(8) The Principal Cyber Advisor of the Department of Defense.

(9) The Principal Cyber Advisors of the military departments.

(10) Each senior official identified pursuant to subsection (i) of section 1647 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1118).

(11) Such other officials as may be determined necessary by the Secretary of Defense.

(c) PROGRAM OFFICE.—(1) There is in the Cybersecurity Directorate of the National Security Agency a program office to support the Program by identifying threats to, vulnerabilities in, and remediations for, the missions and mission elements specified in subsection (d)(1). Such program office shall be headed by a program manager selected by the Director of the National Security Agency.

(2) The Chief Information Officer of the Department of Defense, in exercising authority, direction, and control over the Cybersecurity Directorate of the National Security Agency, shall ensure that the program office under paragraph (1) is responsive to the requirements and direction of the program manager selected pursuant to such paragraph.

(3) The Secretary may augment the personnel assigned to the program office under paragraph (1) by assigning personnel as appropriate from among members of any covered armed force (including the reserve components thereof), civilian employees of the Department of Defense (including the Defense Intelligence Agency), and personnel of the research laboratories of the Department of Defense, who have particular expertise in the areas of responsibility referred to in subsection (d).

(d) DESIGNATION OF MISSION ELEMENTS OF PROGRAM.—(1) The Under Secretary of Defense for Policy, the Under Secretary of Defense for Acquisition and Sustainment, and the Vice Chairman of the Joint Chiefs of Staff shall identify and designate for inclusion in the Program all of the systems, critical infrastructure, kill chains, and processes, including systems and components in development, that comprise the following military missions of the Department of Defense:

(A) Nuclear deterrence and strike.

(B) Select long-range conventional strike missions germane to the warfighting plans of the United States European Command and the United States Indo-Pacific Command.

(C) Offensive cyber operations.

(D) Homeland missile defense.

(2) The Vice Chairman of the Joint Chiefs of Staff shall coordinate the identification and prioritization of the missions and mission components, and the development and approval of requirements relating to the cybersecurity of the missions and mission components, of the Program.

(e) ADDITIONAL RESPONSIBILITIES OF HEAD OF OFFICE OF PRIMARY RESPONSIBILITY.—In addition to providing policy, direction, and oversight as specified in subsection (a)(2), the head of the office of primary responsibility for the Program designated under such subsection shall be responsible—

(1) for overseeing and providing direction on any covered statutory requirement that is ongoing, recurrent (including on an annual basis), or unfulfilled, including by—

(A) reviewing any materials required to be submitted to Congress under the covered statutory requirement prior to such submission; and

(B) ensuring such submissions occur by the applicable deadline under the covered statutory requirement; and

(2) recording and monitoring the remediation of identified vulnerabilities in constituent systems, infrastructure, kill chains, and processes of the missions specified in subsection (d)(1).

(f) RESPONSIBILITIES OF PROGRAM MANAGER.—The program manager selected pursuant to subsection (c)(1) shall be responsible for the following:

(1) Conducting end-to-end vulnerability assessments of the constituent systems, infrastructure, kill chains, and processes of the missions specified in subsection (d)(1).

(2) Prioritizing and facilitating the remediation of identified vulnerabilities in such constituent systems, infrastructure, kill chains, and processes.

(3) Conducting, prior to the Milestone B approval for any proposed such system or infrastructure germane to the missions of the Program, appropriate reviews of the acquisition and system engineering plans for that proposed system or infrastructure, in accordance with the policy and guidance of the Under Secretary of Defense for Acquisition and Sustainment regarding the components of such reviews and the range of systems and infrastructure to be reviewed.

(4) Advising the Secretaries of the military departments, the commanders of the combatant commands, and the Joint Staff on the vulnerabilities and cyberattack vectors that pose substantial risk to the missions of the Program and their constituent systems, critical infrastructure, kill chains, or processes.

(5) Ensuring that the Program builds upon (including through the provision of oversight and direction by the head of the office of primary responsibility for the Program pursuant to subsection (e), as applicable), and does not duplicate, other efforts of the Department of Defense relating to cybersecurity, including the following:

(A) The evaluation of cyber vulnerabilities of major weapon systems of the Department of Defense required under section 1647 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1118).

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

(C) The activities of the cyber protection teams of the Department of Defense.

(g) RESPONSIBILITIES OF SECRETARY OF DEFENSE.—The Secretary of Defense shall define and issue guidance on the roles and responsibilities for components of the Department of Defense other than those specified in this section with respect to the Program, including—

(1) the roles and responsibilities of the acquisition and sustainment organizations of the military departments in supporting and implementing remedial actions;

(2) the alignment of Cyber Protection Teams with the prioritized missions of the Program;

(3) the role of the Director of Operational Test and Evaluation in conducting periodic assessments, including through cyber red teams, of the cybersecurity of missions in the Program; and

(4) the role of the Principal Cyber Adviser in coordinating and monitoring the execution of the Program.

(h) ANNUAL REPORTING.—Not later than December 31 of each year, the head of the office of primary responsibility for the Program, in coordination with the appropriate members of the Program under subsection (b), shall submit to the congressional defense committees an annual report on the efforts carried out pursuant to this section or any covered provision of law, including with respect to such efforts concerning—

(1) the evaluation of cyber vulnerabilities of each major weapon system of the Department of Defense and related mitigation activities under section 1647 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1118);

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

(3) operational technology and the mapping of mission-relevant terrain in cyberspace under section 1505 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81; 10 U.S.C. 394 note);

(4) the 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 under section 1559 of the National Defense Authorization Act for Fiscal Year 2023; and

(5) the work of the Program in general, including information relating to staffing and accomplishments.

(i) ANNUAL BUDGET DISPLAY.—(1) On an annual basis for each fiscal year, concurrently with the submission of the budget of the President for that fiscal year under section 1105(a) of title 31, United States Code, the head of the office of primary responsibility for the Program, in coordination with the appropriate members of the Program under subsection (b), shall submit to the congressional defense committees a consolidated budget justification display that covers all programs and activities associated with this section and any covered provision of law, including with respect to the matters listed in subsection (h).

(2) Each display under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(3) For the purpose of facilitating the annual budget display requirement under paragraph (1), the Chief Information Officer of the Department of Defense shall provide to the head of the office of primary responsibility for the Program and the appropriate members of the Program under subsection (b) fiscal guidance on the programming of funds in support of the Program.

(j) DEFINITIONS.—In this section:

(1) The term ''covered armed force'' means the Army, Navy, Air Force, Marine Corps, or Space Force.

(2) The term ''covered statutory requirement'' means a requirement under any covered provision of law.

(3) The term ''covered provision of law'' means the following:

(A) Section 1647 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1118).

(B) Section 1650 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 10 U.S.C. 2224 note).

(C) Section 1505 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81; 10 U.S.C. 394 note).

(D) Section 1559 of the National Defense Authorization Act for Fiscal Year 2023.

(Added Pub. L. 118–31, div. A, title XV, § 1502(a)(1), Dec. 22, 2023, 137 Stat. 533; amended Pub. L. 118–159, div. A, title XVII, § 1701(a)(7), Dec. 23, 2024, 138 Stat. 2203.)

Editorial Notes

REFERENCES IN TEXT

Section 1647 of the National Defense Authorization Act for Fiscal Year 2016, referred to in subsecs. (b)(10), (f)(5)(A), (h)(1), and (j)(3)(A), is section 1647 of Pub. L. 114–92, which is set out as a note under section 2224 of this title.

Section 1559 of the National Defense Authorization Act for Fiscal Year 2023, referred to in subsecs. (h)(4) and (j)(3)(D), is section 1559 of Pub. L. 117–263, which is set out as a note under section 2224 of this title.

AMENDMENTS

2024—Subsec. (e)(1)(B). Pub. L. 118–159 substituted semicolon for colon after ''requirement''.

§ 392. Executive agents for cyber test and training ranges

(a) EXECUTIVE AGENT.—The Secretary of Defense, in consultation with the Principal Cyber Advisor, shall—

(1) designate a senior official from among the personnel of the Department of Defense to act as the executive agent for cyber and information technology test ranges; and

(2) designate a senior official from among the personnel of the Department of Defense to act as the executive agent for cyber and information technology training ranges.

(b) ROLES, RESPONSIBILITIES, AND AUTHORITIES.—

(1) ESTABLISHMENT.—The Secretary of Defense shall prescribe the roles, responsibilities, and authorities of the executive agents designated under subsection (a). Such roles, responsibilities, and authorities shall include the development of a biennial integrated plan for cyber and information technology test and training resources.

(2) BIENNIAL INTEGRATED PLAN.—The biennial integrated plan required under paragraph (1) shall include plans for the following:

(A) Developing and maintaining a comprehensive list of cyber and information technology ranges, test facilities, test beds, and other means of testing, training, and developing software, personnel, and tools for accommodating the mission of the Department. Such list shall include resources from both governmental and nongovernmental entities.

(B) Organizing and managing designated cyber and information technology test ranges, including—

(i) establishing the priorities for cyber and information technology ranges to meet Department objectives;

(ii) enforcing standards to meet requirements specified by the United States Cyber Command, the training community, and the research, development, testing, and evaluation community;

(iii) identifying and offering guidance on the opportunities for integration amongst the designated cyber and information technology ranges regarding test, training, and development functions;

(iv) finding opportunities for cost reduction, integration, and coordination improvements for the appropriate cyber and information technology ranges;

(v) adding or consolidating cyber and information technology ranges in the future to better meet the evolving needs of the cyber strategy and resource requirements of the Department;

(vi) finding opportunities to continuously enhance the quality and technical expertise of the cyber and information technology test workforce through training and personnel policies; and

(vii) coordinating with interagency and industry partners on cyber and information technology range issues.

(C) Defining a cyber range architecture that—

(i) may add or consolidate cyber and information technology ranges in the future to better meet the evolving needs of the cyber strategy and resource requirements of the Department;

(ii) coordinates with interagency and industry partners on cyber and information technology range issues;

(iii) allows for integrated closed loop testing in a secure environment of cyber and electronic warfare capabilities;

(iv) supports science and technology development, experimentation, testing and training; and

(v) provides for interconnection with other existing cyber ranges and other kinetic range facilities in a distributed manner.

(D) Certifying all cyber range investments of the Department of Defense.

(E) Performing such other assessments or analyses as the Secretary considers appropriate.

(3) STANDARD FOR CYBER EVENT DATA.—The executive agents designated under subsection (a), in consultation with the Chief Information Officer of the Department of Defense, shall jointly select a standard language from open-source candidates for representing and communicating cyber event and threat data. Such language shall be machine-readable for the Joint Information Environment and associated test and training ranges.