(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.

(c) SUPPORT WITHIN DEPARTMENT OF DEFENSE.—The Secretary of Defense shall ensure that the military departments, Defense Agencies, and other components of the Department of Defense provide the executive agents designated under subsection (a) with the appropriate support and resources needed to perform the roles, responsibilities, and authorities of the executive agents.

(d) COMPLIANCE WITH EXISTING DIRECTIVE.—The Secretary shall carry out this section in compliance with Directive 5101.1.

(e) DEFINITIONS.—In this section:

(1) The term ''designated cyber and information technology range'' includes the National Cyber Range, the Joint Information Operations Range, the Defense Information Assurance Range, and the C4 Assessments Division of J6 of the Joint Staff.

(2) The term ''Directive 5101.1'' means Department of Defense Directive 5101.1, or any successor directive relating to the responsibilities of an executive agent of the Department of Defense.

(3) The term ''executive agent'' has the meaning given the term ''DoD Executive Agent'' in Directive 5101.1.

(Added Pub. L. 113–291, div. A, title XVI, §1633(a), Dec. 19, 2014, 128 Stat. 3641.)

Statutory Notes and Related Subsidiaries

DESIGNATION AND ROLES AND RESPONSIBILITIES; SELECTION OF STANDARD LANGUAGE

Pub. L. 113–291, div. A, title XVI, §1633(b), (c), Dec. 19, 2014, 128 Stat. 3642, provided that:

''(b) DESIGNATION AND ROLES AND RESPONSIBILITIES.—The Secretary of Defense shall—

''(1) not later than 120 days after the date of the enactment of this Act [Dec. 19, 2014], designate the executive agents required under subsection (a) of section 392 of title 10, United States Code, as added by subsection (a) of this section; and

''(2) not later than one year after the date of the enactment of this Act, prescribe the roles, responsibilities, and authorities required under subsection (b) of such section 392.

''(c) SELECTION OF STANDARD LANGUAGE.—Not later than June 1, 2015, the executive agents designated under subsection (a) of section 392 of title 10, United States Code, as added by subsection (a) of this section, shall select the standard language under subsection (b)(3) of such section 392.''

§ 392a. Principal Cyber Advisors

(a) PRINCIPAL CYBER ADVISOR TO SECRETARY OF DEFENSE.—

(1) ESTABLISHMENT.—There is a Principal Cyber Advisor in the Department of Defense.

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

(A) Acting as the principal advisor to the Secretary on military cyber forces and activities.

(B) Overall integration of Cyber Operations Forces activities relating to cyberspace operations, including associated policy and operational considerations, resources, personnel, technology development and transition, and acquisition.

(C) Assessing and overseeing the implementation of the cyber strategy of the Department and execution of the cyber posture review of the Department on behalf of the Secretary.

(D) Coordinating activities pursuant to subparagraphs (A) and (B) of paragraph (3) with the Principal Information Operations Advisor, the Chief Information Officer of the Department, and other officials as determined by the Secretary of Defense, to ensure the integration of activities in support of cyber, information, and electromagnetic spectrum operations.

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

(3) CROSS-FUNCTIONAL TEAM.—Consistent with section 911 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 10 U.S.C. 111 note), the Principal Cyber Advisor shall—

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

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

(4) BUDGET REVIEW.—(A) The Secretary of Defense, acting through the Under Secretary of Defense (Comptroller), shall require the Secretaries of the military departments and the heads of the Defense agencies with responsibilities associated with any activity specified in paragraph (2) to transmit the proposed budget for such activities for a fiscal year and for the period covered by the future-years defense program submitted to Congress under section 221 of this title for that fiscal year to the Principal Cyber Advisor for review under subparagraph (B) before submitting the proposed budget to the Under Secretary of Defense (Comptroller).

(B) The Principal Cyber Advisor shall review each proposed budget transmitted under subparagraph (A) and, not later than January 31 of the year preceding the fiscal year for which the budget is proposed, shall submit to the Secretary of Defense a report containing the comments of the Principal Cyber Advisor with respect to all such proposed budgets, together with the certification of the Principal Cyber Advisor regarding whether each proposed budget is adequate.

(C) Not later than March 31 of each year, the Secretary of Defense shall submit to Congress a report specifying each proposed budget that the Principal Cyber Advisor did not certify to be adequate. The report of the Secretary shall include the following matters:

(i) A discussion of the actions that the Secretary proposes to take, together with any recommended legislation that the Secretary considers appropriate, to address the