(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

inadequacy of the proposed budgets specified in the report.

(ii) Any additional comments that the Secretary considers appropriate regarding the inadequacy of the proposed budgets.

(b) SENIOR MILITARY ADVISOR FOR CYBER POLICY AND DEPUTY PRINCIPAL CYBER ADVISOR.—

(1) ADVISOR.—

(A) IN GENERAL.—The Secretary of Defense shall, acting through the Joint Staff, designate an officer within the Office of the Under Secretary of Defense for Policy to serve within that Office as the Senior Military Advisor for Cyber Policy, and concurrently, as the Deputy Principal Cyber Advisor.

(B) OFFICERS ELIGIBLE FOR DESIGNATION.—The officer designated pursuant to this paragraph shall be designated from among commissioned regular officers of the Armed Forces in a general or flag officer grade who are qualified for designation.

(C) GRADE.—The officer designated pursuant to this paragraph shall have the grade of major general or rear admiral (upper half) while serving in that position, without vacating the officer's permanent grade.

(2) SCOPE OF POSITIONS.—

(A) IN GENERAL.—The officer designated pursuant to paragraph (1) is each of the following:

(i) The Senior Military Advisor for Cyber Policy to the Under Secretary of Defense for Policy.

(ii) The Deputy Principal Cyber Advisor to the Secretary of Defense.

(B) DIRECTION AND CONTROL AND REPORTING.—In carrying out duties under this section, the officer designated pursuant to paragraph (1) shall be subject to the authority, direction, and control of, and shall report directly to, the following:

(i) The Under Secretary with respect to Senior Military Advisor for Cyber Policy duties.

(ii) The Principal Cyber Advisor with respect to Deputy Principal Cyber Advisor duties.

(3) DUTIES.—

(A) DUTIES AS SENIOR MILITARY ADVISOR FOR CYBER POLICY.—The duties of the officer designated pursuant to paragraph (1) as Senior Military Advisor for Cyber Policy are as follows:

(i) To serve as the principal uniformed military advisor on military cyber forces and activities to the Under Secretary of Defense for Policy.

(ii) To assess and advise the Under Secretary on aspects of policy relating to military cyberspace operations, resources, personnel, cyber force readiness, cyber workforce development, and defense of Department of Defense networks.

(iii) To advocate, in consultation with the Joint Staff, and senior officers of the Armed Forces and the combatant commands, for consideration of military issues within the Office of the Under Secretary of Defense for Policy, including coordination and synchronization of Department cyber forces and activities.

(iv) To maintain open lines of communication between the Chief Information Officer of the Department of Defense, senior civilian leaders within the Office of the Under Secretary, and senior officers on the Joint Staff, the Armed Forces, and the combatant commands on cyber matters, and to ensure that military leaders are informed on cyber policy decisions.

(B) DUTIES AS DEPUTY PRINCIPAL CYBER ADVISOR.—The duties of the officer designated pursuant to paragraph (1) as Deputy Principal Cyber Advisor are as follows:

(i) To synchronize, coordinate, and oversee implementation of the Cyber Strategy of the Department of Defense and other relevant policy and planning.

(ii) To advise the Secretary of Defense on cyber programs, projects, and activities of the Department, including with respect to policy, training, resources, personnel, manpower, and acquisitions and technology.

(iii) To oversee implementation of Department policy and operational directives on cyber programs, projects, and activities, including with respect to resources, personnel, manpower, and acquisitions and technology.

(iv) To assist in the overall supervision of Department cyber activities relating to offensive missions.

(v) To assist in the overall supervision of Department defensive cyber operations, including activities of component-level cybersecurity service providers and the integration of such activities with activities of the Cyber Mission Force.

(vi) To advise senior leadership of the Department on, and advocate for, investment in capabilities to execute Department missions in and through cyberspace.

(vii) To identify shortfalls in capabilities to conduct Department missions in and through cyberspace, and make recommendations on addressing such shortfalls in the Program Budget Review process.

(viii) To coordinate and consult with stakeholders in the cyberspace domain across the Department in order to identify other issues on cyberspace for the attention of senior leadership of the Department.

(ix) On behalf of the Principal Cyber Advisor, to lead the cross-functional team established pursuant to section 932(c)(3) of the National Defense Authorization Act for Fiscal Year 2014 (10 U.S.C. 2224 note)[1] in order to synchronize and coordinate military and civilian cyber forces and activities of the Department.

(c) CYBER GOVERNANCE STRUCTURES AND PRINCIPAL CYBER ADVISORS ON MILITARY CYBER FORCE MATTERS.—

[1] See References in Text note below.

(1) DESIGNATION.—

(A) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, each of the secretaries of the military departments, in consultation with the service chiefs, shall appoint an independent Principal Cyber Advisor for each service to act as the principal advisor to the relevant secretary on all cyber matters affecting that military service.

(B) NATURE OF POSITION.—Each Principal Cyber Advisor position under subparagraph (A) shall—

(i) be a senior civilian leadership position, filled by a senior member of the Senior Executive Service, not lower than the equivalent of a 3-star general officer, or by exception a comparable military officer with extensive cyber experience;

(ii) exclusively occupy the Principal Cyber Advisor position and not assume any other position or responsibility in the relevant military department;

(iii) be independent of the relevant service's chief information officer; and

(iv) report directly to and advise the secretary of the relevant military department and advise the relevant service's senior uniformed officer.

(C) NOTIFICATION.—Each of the secretaries of the military departments shall notify the Committees on Armed Services of the Senate and House of Representatives of his or her Principal Cyber Advisor appointment. In the case that the appointee is a military officer, the notification shall include a justification for the selection and an explanation of the appointee's ability to execute the responsibilities of the Principal Cyber Advisor.

(2) RESPONSIBILITIES OF PRINCIPAL CYBER ADVISORS.—Each Principal Cyber Advisor under paragraph (1) shall be responsible for advising both the secretary of the relevant military department and the senior uniformed military officer of the relevant military service and implementing the Department of Defense Cyber Strategy within the service by coordinating and overseeing the execution of the service's policies and programs relevant to the following:

(A) The recruitment, resourcing, and training of military cyberspace operations forces, assessment of these forces against standardized readiness metrics, and maintenance of these forces at standardized readiness levels.

(B) Acquisition of offensive, defensive, and Department of Defense Information Networks cyber capabilities for military cyberspace operations.

(C) Cybersecurity management and operations.

(D) Acquisition of cybersecurity tools and capabilities, including those used by cybersecurity service providers.

(E) Evaluating, improving, and enforcing a culture of cybersecurity warfighting and accountability for cybersecurity and cyberspace operations.

(F) Cybersecurity and related supply chain risk management of the industrial base.

(G) Cybersecurity of Department of Defense information systems, information technology services, and weapon systems, including the incorporation of cybersecurity threat information as part of secure development processes, cybersecurity testing, and the mitigation of cybersecurity risks.

(3) COORDINATION.—To ensure service compliance with the Department of Defense Cyber Strategy, each Principal Cyber Advisor under paragraph (1) shall work in close coordination with the following:

(A) Service chief information officers.

(B) Service cyber component commanders.

(C) Principal Cyber Advisor to the Secretary of Defense.

(D) Department of Defense Chief Information Officer.

(E) Defense Digital Service.

(4) BUDGET CERTIFICATION AUTHORITY.—

(A) IN GENERAL.—Each of the secretaries of the military departments shall require service components with responsibilities associated with cyberspace operations forces, offensive or defensive cyberspace operations and capabilities, and cyberspace issues relevant to the duties specified in paragraph (2) to transmit the proposed budget for such responsibilities for a fiscal year and for the period covered by the future-years defense program submitted to Congress under section 221 of title 10, United States Code, for that fiscal year to the relevant service's Principal Cyber Advisor for review under subparagraph (B) before submitting the proposed budget to the department's comptroller.

(B) REVIEW.—Each Principal Cyber Advisor under paragraph (1)(A) shall review each proposed budget transmitted under subparagraph (A) and submit to the secretary of the relevant military department 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) REPORT.—Not later than March 31 of each year, each of the secretaries of the military departments shall submit to the congressional defense committees a report specifying each proposed budget for the subsequent fiscal year contained in the most-recent report submitted under subparagraph (B) that the Principal Cyber Advisor did not certify to be adequate. The report of the secretary shall include a discussion of the actions that the secretary took or proposes to take, together with any additional comments that the Secretary considers appropriate regarding the adequacy or inadequacy of the proposed budgets.

(5) PRINCIPAL CYBER ADVISORS' BRIEFING TO CONGRESS.—Not later than February 1, 2021, and biannually thereafter, each Principal Cyber Advisor under paragraph (1) shall brief the Committees on Armed Services of the Senate and House of Representatives on that Ad-

visor's activities and ability to perform the functions specified in paragraph (2).

(Added and amended Pub. L. 117–263, div. A, title XV, §1501(b), Dec. 23, 2022, 136 Stat. 2877; Pub. L. 118–31, div. A, title XVIII, §1801(a)(5), Dec. 22, 2023, 137 Stat. 683; Pub. L. 118–159, div. A, title XVII, §1701(a)(8), Dec. 23, 2024, 138 Stat. 2203.)

Editorial Notes

REFERENCES IN TEXT

Section 911 of the National Defense Authorization Act for Fiscal Year 2017, referred to in subsec. (a)(3), is section 911 of Pub. L. 114–328, which is set out as a note under section 111 of this title.

Section 932(c)(3) of the National Defense Authorization Act for Fiscal Year 2014, referred to in subsec. (b)(3)(B)(ix), is section 932(c)(3) of Pub. L. 113–66, which was formerly set out as a note under section 2224 of this title and was transferred to this section and redesignated as subsec. (a)(3) by Pub. L. 117–263, §1501(b)(2)(A), (B), Dec. 23, 2022, 136 Stat. 2878.

The date of the enactment of this Act, referred to in subsec. (c)(1)(A), means the date of enactment of Pub. L. 116–92, which had originally enacted the text of subsec. (c) of this section and was approved Dec. 20, 2019. See Codification note below.

CODIFICATION

The text of section 932(c) of Pub. L. 113–66, formerly set out as a note under section 2224 of this title, which was transferred to this section, redesignated as subsec. (a), and amended by Pub. L. 117–263, §1501(b)(2), was based on 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), Dec. 23, 2022, 136 Stat. 2797, 2877.

The text of section 905 of Pub. L. 116–92, formerly set out as a note under section 391 of this title, which was transferred to this section, redesignated as subsec. (b), and amended by Pub. L. 117–263, §1501(b)(3), was based on Pub. L. 116–92, div. A, title IX, §905, Dec. 20, 2019, 133 Stat. 1557, as amended by Pub. L. 116–283, div. A, title XVII, §1713(b), Jan. 1, 2021, 134 Stat. 4090; Pub. L. 117–81, div. A, title XV, §1503(b), Dec. 27, 2021, 135 Stat. 2021; Pub. L. 117–263, div. A, title X, §1081(c), Dec. 23, 2022, 136 Stat. 2797.

The text of section 1657 of Pub. L. 116–92, formerly set out as a note under section 391 of this title, which was transferred to this section, redesignated as subsec. (c), and amended by Pub. L. 117–263, §1501(b)(4), was based on Pub. L. 116–92, div. A, title XVI, §1657, Dec. 20, 2019, 133 Stat. 1767.

AMENDMENTS

2024—Subsec. (b)(3)(B)(ix). Pub. L. 118–159 inserted ''section'' before ''932(c)(3)''.

2023—Subsec. (b)(2)(B). Pub. L. 118–31, §1801(a)(5)(A), substituted ''designated'' for ''designed'' in introductory provisions.

Subsec. (c)(4)(A). Pub. L. 118–31, §1801(a)(5)(B), substituted ''subparagraph (B)'' for ''clause (ii)''.

2022—Subsec. (a). Pub. L. 117–263, §1501(b)(2)(A), (B), (D), transferred section 932(c) of Pub. L. 113–66 to this section, redesignated it as subsec. (a), and inserted ''to Secretary of Defense'' after ''Advisor'' in heading. See Codification note above.

Subsec. (a)(1). Pub. L. 117–263, §1501(b)(2)(C), added par. (1) and struck out former par. (1) which related to designation of a Principal Cyber Advisor by the Secretary of Defense.

Subsec. (b). Pub. L. 117–263, §1501(b)(3)(A), transferred section 905 of Pub. L. 116–92 to this section, redesignated it as subsec. (b), redesignated each subordinate provision to conform to such redesignation, and realigned margins. See Codification note above.

Subsec. (b)(1)(B), (C). Pub. L. 117–263, §1501(b)(3)(B)(i), substituted ''this paragraph'' for ''this subsection''.

Subsec. (b)(2), (3). Pub. L. 117–263, §1501(b)(3)(B)(ii), substituted ''paragraph (1)'' for ''subsection (a)'' in introductory provisions of subpars. (A) and (B).

Subsec. (c). Pub. L. 117–263, §1501(b)(4)(A), transferred section 1657 of Pub. L. 116–92 to this section, redesignated it as subsec. (c), redesignated each subordinate provision to conform to such redesignation, and realigned margins. See Codification note above.

Subsec. (c)(1)(B). Pub. L. 117–263, §1501(b)(4)(B)(ii), substituted ''subparagraph (A)'' for ''paragraph (1)'' in introductory provisions.

Subsec. (c)(2), (3). Pub. L. 117–263, §1501(b)(4)(B)(v), substituted ''paragraph (1)'' for ''subsection (a)'' in introductory provisions.

Subsec. (c)(4)(A). Pub. L. 117–263, §1501(b)(4)(B)(i), (vi), substituted ''paragraph (2)'' for ''subsection (b)'' and ''clause (ii)'' for ''subparagraph (B)''.

Subsec. (c)(4)(B). Pub. L. 117–263, §1501(b)(4)(B)(ii), (iv), substituted ''paragraph (1)(A)'' for ''subsection (a)(1)'' and ''subparagraph (A)'' for ''paragraph (1)''.

Subsec. (c)(4)(C). Pub. L. 117–263, §1501(b)(4)(B)(iii), substituted ''subparagraph (B)'' for ''paragraph (2)''.

Subsec. (c)(5). Pub. L. 117–263, §1501(b)(4)(B)(v), (vi), substituted ''paragraph (1)'' for ''subsection (a)'' and ''paragraph (2)'' for ''subsection (b)''.

Subsec. (c)(6). Pub. L. 117–263, §1501(b)(4)(B)(vii), struck out par. (6) which authorized each of the secretaries of the military departments to review relevant military department's current governance model for cybersecurity with respect to current authorities and responsibilities.

Subsec. (c)(6)(B). Pub. L. 117–263, §1501(b)(4)(B)(ii), (v), substituted ''subparagraph (A)'' for ''paragraph (1)'' in introductory provisions and ''paragraph (1)'' for ''subsection (a)'' in cl. (i).

Subsec. (c)(6)(C). Pub. L. 117–263, §1501(b)(4)(B)(ii), substituted ''subparagraph (A)'' for ''paragraph (1)''.

§ 393. Reporting on penetrations of networks and information systems of certain contractors

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

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

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

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

(A) The Under Secretary of Defense for Policy.

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

(C) the Under Secretary of Defense for Research and Engineering.

(D) The Under Secretary of Defense for Intelligence and Security.

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

(F) The Commander of the United States Cyber Command.

(c) PROCEDURE REQUIREMENTS.—