§ 167b. Unified combatant command for cyber operations

(a) ESTABLISHMENT.—(1) With the advice and assistance of the Chairman of the Joint Chiefs of Staff, the President, through the Secretary of Defense, shall establish under section 161 of this title a unified combatant command for cyber operations forces (hereinafter in this section referred to as the ''United States Cyber Command'').

(2) The principal mission of the United States Cyber Command is to direct, synchronize, and coordinate military cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners.

(b) ASSIGNMENT OF FORCES.—(1) Active and reserve cyber forces of the armed forces shall be assigned to the United States Cyber Command through the Global Force Management Process, as approved by the Secretary of Defense.

(2) Cyber forces not assigned to United States Cyber Command remain assigned to combatant commands or service-retained.

(c) GRADE OF COMMANDER.—The Commander of the United States Cyber Command shall hold the grade of general or, in the case of an officer of the Navy, admiral while serving in that position, without vacating that officer's permanent grade. The Commander of such Command shall be appointed to that grade by the President, by and with the advice and consent of the Senate, for service in that position.

(d) AUTHORITY OF COMBATANT COMMANDER.—(1) In addition to the authority prescribed in section 164(c) of this title, the Commander of the United States Cyber Command shall be responsible for, and shall have the authority to conduct, all affairs of such Command relating to cyber operations activities.

(2)(A) Subject to the authority, direction, and control of the Principal Cyber Advisor to the Secretary of Defense under section 392a(a) of this title, the Commander of such Command shall be responsible for, and shall have the authority to conduct, the following functions relating to cyber operations activities (whether or not relating to the United States Cyber Command):

(i) Developing strategy, doctrine, and tactics.

(ii) Preparing and submitting to the Secretary of Defense program recommendations and budget proposals for cyber operations forces and for other forces assigned to the United States Cyber Command.

(iii) Exercising authority, direction, and control over the expenditure of funds—

(I) for forces assigned directly to the United States Cyber Command; and

(II) for cyber operations forces assigned to unified combatant commands other than the United States Cyber Command, with respect to all matters covered by section 807 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 886; 10 U.S.C. 2224 note) and, with respect to a matter not covered by such section, to the extent directed by the Secretary of Defense.

(iv) Training and certification of assigned joint forces.

(v) Conducting specialized courses of instruction for commissioned and noncommissioned officers.

(vi) Validating requirements.

(vii) Establishing priorities for requirements.

(viii) Ensuring the interoperability of equipment and forces.

(ix) Formulating and submitting requirements for intelligence support.

(x) Monitoring the promotion of cyber operation forces and coordinating with the military departments regarding the assignment, retention, training, professional military education, and special and incentive pays of cyber operation forces.

(B) The authority, direction, and control exercised by the Principal Cyber Advisor for purposes of this section is authority, direction, and control with respect to the administration and support of the United States Cyber Command, including readiness and organization of cyber operations forces, cyber operations-peculiar equipment and resources, and civilian personnel.

(C) Nothing in this section shall be construed as providing the Principal Cyber Advisor authority, direction, and control of operational matters that are subject to the operational chain of command of the combatant commands or the exercise of authority, direction, and control of personnel, resources, equipment, and other matters that are not cyber-operations peculiar and that are in the purview of the armed forces.

(3) The Commander of the United States Cyber Command shall be responsible for—

(A) ensuring the combat readiness of forces assigned to the United States Cyber Command; and

(B) monitoring the preparedness to carry out assigned missions of cyber forces assigned to unified combatant commands other than the United States Cyber Command.

(C) The staff of the Commander shall include an inspector general who shall conduct internal audits and inspections of purchasing and contracting actions through the cyber operations command and such other inspector general functions as may be assigned.

(e) INTELLIGENCE AND SPECIAL ACTIVITIES.—This section does not 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.).

(Added Pub. L. 114–328, div. A, title IX, §923(a), Dec. 23, 2016, 130 Stat. 2357; amended Pub. L. 115–91, div. A, title X, §1081(a)(12), title XVI, §1635, Dec. 12, 2017, 131 Stat. 1595, 1741; Pub. L. 116–283, div. A, title XVII, §1701(1), Jan. 1, 2021, 134 Stat. 4079; Pub. L. 117–263, div. A, title XV, §1501(c)(1), Dec. 23, 2022, 136 Stat. 2878; Pub. L. 118–159, div. A, title XVII, §1701(a)(4), Dec. 23, 2024, 138 Stat. 2203.)

Editorial Notes

REFERENCES IN TEXT

The National Security Act of 1947, referred to in subsec. (e), is act July 26, 1947, ch. 343, 61 Stat. 495. Title V of the Act is classified generally to subchapter III (§3091 et seq.) of chapter 44 of Title 50. For complete classification of this Act to the Code, see Tables.

AMENDMENTS

2024—Subsec. (a)(1). Pub. L. 118–159, §1701(a)(4)(A)(i), substituted ''referred to as the 'United States Cyber Command' '' for ''referred to as the 'cyber command' ''.

Subsec. (a)(2). Pub. L. 118–159, §1701(a)(4)(A)(ii), substituted ''United States Cyber Command'' for ''Cyber Command''.

Subsec. (b). Pub. L. 118–159, §1701(a)(4)(B), substituted ''United States Cyber Command'' for ''Cyber Command'' in pars. (1) and (2).

Subsec. (c). Pub. L. 118–159, §1701(a)(4)(C), substituted ''Commander'' for ''commander'' in two places, ''United States Cyber Command'' for ''cyber command'', and ''such Command'' for ''such command''.

Subsec. (d). Pub. L. 118–159, §1701(a)(4)(C), substituted ''Commander'' for ''commander'' and ''United States Cyber Command'' for ''cyber command'' wherever appearing and ''such Command'' for ''such command'' in two places.

2022—Subsec. (d)(2)(A). Pub. L. 117–263 inserted ''to the Secretary of Defense under section 392a(a) of this title'' after ''Principal Cyber Advisor'' in introductory provisions.

2021—Subsec. (a). Pub. L. 116–283, §1701(1)(A), designated existing provisions as par. (1), struck out at end ''The principal function of the command is to prepare cyber operations forces to carry out assigned missions.'', and added par. (2).

Subsec. (b). Pub. L. 116–283, §1701(1)(B), amended subsec. (b) generally. Prior to amendment, text read as follows: ''Unless otherwise directed by the Secretary of Defense, all active and reserve cyber operations forces of the armed forces stationed in the United States shall be assigned to the cyber command.''

2017—Subsec. (d). Pub. L. 115–91, §1635, redesignated subsec. (e) as (d) and struck out former subsec. (d) which related to command of activity or mission.

Subsec. (e). Pub. L. 115–91, §1635(2), redesignated subsec. (f) as (e). Former subsec. (e) redesignated (d).

Subsec. (e)(2)(A)(iii)(II). Pub. L. 115–91, §1081(a)(12), substituted ''Fiscal Year 2016'' for ''Fiscal Year 2014''.

Subsec. (f). Pub. L. 115–91, §1635(2), redesignated subsec. (f) as (e).

Statutory Notes and Related Subsidiaries

DEPARTMENT OF DEFENSE INFORMATION NETWORK SUBORDINATE UNIFIED COMMAND

Pub. L. 118–159, div. A, title XV, §1502, Dec. 23, 2024, 138 Stat. 2131, provided that:

''(a) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act [Dec. 23, 2024], the Secretary of Defense shall designate the Joint Force Headquarters-Department of Defense Information Network as a subordinate unified command under the United States Cyber Command.

''(b) DESIGNATION NOTICE.—On the date on which the Secretary of Defense makes the designation required by subsection (a), the Secretary shall issue to the Secretary of each military department (as defined in section 101(a) of title 10, United States Code), the Chairman of the Joint Chiefs of Staff, the Under Secretaries of the Department of Defense, the Chief of the National Guard Bureau, the General Counsel of the Department of Defense, the Director of Cost Assessment and Program Evaluation, the Inspector General of the Department of Defense, the Director of Operational Test and Evaluation, the Chief Information Officer of the Department of Defense, the Assistant Secretary of Defense for Legislative Affairs, the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, the Chief Digital and Artificial Intelligence Officer of the Department of Defense, the commander of each combatant command, and the head of each Defense Agency and Department of Defense Field Activity (as such terms are defined, respectively, in section 101(a) of title 10, United States Code) a notice regarding—

''(1) the designation of the Joint Force Headquarters-Department of Defense Information Network as a subordinate unified command under the United States Cyber Command; and

''(2) the mission of the Joint Force Headquarters-Department of Defense Information Network as the lead organization for the network operations, security, and defense of the Department of Defense Information Network.''

DEVELOPMENT OF CYBER SUPPORT MECHANISMS FOR GEOGRAPHIC COMBATANT COMMANDS

Pub. L. 118–31, div. A, title XV, §1506, Dec. 22, 2023, 137 Stat. 540, provided that:

''(a) DEVELOPMENT OF MECHANISMS REQUIRED.—Not later than 270 days after the date of the enactment of this Act [Dec. 22, 2023], each commander of a geographic combatant command, in coordination with the Commander of the United States Cyber Command, shall develop a cyber support mechanism to support the operations of that geographic combatant command.

''(b) ELEMENTS.—Each cyber support mechanism developed with respect to a geographic combatant command under subsection (a) shall include the following:

''(1) Processes to enhance the cyber capabilities of such combatant command.

''(2) Plans to develop and maintain a sufficient cyber planning capacity in such combatant command.

''(3) Processes to integrate cyber capabilities into operational support for such combatant command.

''(4) A prioritization of cyber risks and vulnerabilities within the geographic area of responsibility of such combatant command.

''(5) Specific plans to assist in the defense of friendly foreign countries.''

PILOT PROGRAM AND OTHER MEASURES TO ENHANCE READINESS AND EFFECTIVENESS OF CYBER MISSION FORCE

Pub. L. 118–31, div. A, title XV, §1535, Dec. 22, 2023, 137 Stat. 566, provided that:

''(a) PERSONNEL REQUIREMENTS AND TRAINING FOR CRITICAL WORK ROLES.—Not later than 270 days after the date of the enactment of this Act [Dec. 22, 2023], the Secretary of Defense shall—

''(1) direct and oversee the implementation of guidance, to be issued by each Secretary of a military department, that correlates critical work roles to military occupational specialties and periods of obligated service with respect to that military department;

''(2) require that, prior to the attachment or assignment of a member of the Armed Forces to a unit of the United States Cyber Command, the Secretary concerned ensure such member is fully trained and in compliance with the required standards for the work role to be assumed by the member within such unit, including with respect to critical work roles within the Cyber Mission Force;

''(3) ensure that the period of obligated service for members of the Armed Forces is—

''(A) uniform across the military departments with respect to positions of the Cyber Mission Force involving critical work roles;

''(B) commensurate with the financial and time investments made by Secretary concerned for the purpose of furnishing training pursuant to paragraph (2); and

''(C) sufficient to meet the readiness requirements established by the Commander of the United States Cyber Command;

''(4) facilitate consecutive assignments of members of the Armed Forces to the same unit of the United States Cyber Command without inhibiting the advancement or promotion potential of any such member;

''(5) provide to the Secretaries of the military departments direction for the integration of critical work roles into the personnel system of record of the respective military department, to provide for tracking cyber personnel data by work role; and

''(6) establish within at least one military department the curriculum and capacity necessary to train sufficient numbers of members of the Armed Forces from across the military departments in the performance of critical work roles within the Cyber Mission Force to achieve the readiness requirements established by the Commander of United States Cyber Command.

''(b) PILOT PROGRAM ON CONTRACTING FOR SERVICES RELEVANT TO CRITICAL WORK ROLES.—

''(1) PILOT PROGRAM.—Not later than 180 days after the date of the enactment of this Act, the Commander of the United States Cyber Command shall carry out a pilot program under which the Commander shall seek to enter into one or more contracts under which skilled contractor personnel provide services relevant to critical work roles within the Cyber Mission Force, for the purpose of enhancing the readiness and effectiveness of the Cyber Mission Force.

''(2) DURATION.—The Commander shall carry out the pilot program under paragraph (1) during the three-year period beginning on the date of the commencement of the pilot program and following such period, may—

''(A) continue carrying out such pilot program for such duration as the Commander considers appropriate;

''(B) transition such pilot program to a permanent program; or

''(C) terminate such pilot program.

''(c) PLAN ON HIRING, TRAINING, AND RETAINING CIVILIANS TO SERVE IN CRITICAL WORK ROLES.—Not later than 120 days after the date of the enactment of this Act, the Commander of the United States Cyber Command shall—

''(1) develop a plan to hire, train, and retain civilians to serve in critical work roles and other work roles within the Cyber Mission Force, for the purpose of enhancing the readiness and effectiveness of the Cyber Mission Force; and

''(2) provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on such plan.

''(d) DEFINITIONS.—In this section:

''(1) The term 'critical work role' means a work role designated as critical by the Commander of the United States Cyber Command for purposes of this section.

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

MANAGEMENT AND OVERSIGHT OF JOINT CYBER WARFIGHTING ARCHITECTURE

Pub. L. 117–263, div. A, title XV, §1509, Dec. 23, 2022, 136 Stat. 2886, provided that:

''(a) ESTABLISHMENT OF OFFICES.—

''(1) REQUIREMENT.—The Secretary of Defense, in consultation with the Commander of the United States Cyber Command, shall establish within the United States Cyber Command—

''(A) a program executive office; and

''(B) one or more subordinate program management offices under the program executive office.

''(2) RESPONSIBILITIES.—The offices established pursuant to paragraph (1) shall—

''(A) oversee, manage, and execute the Joint Cyber Warfighting Architecture;

''(B) oversee, manage, and execute the programs designated, or to be designated, as part of the Joint Cyber Warfighting Architecture;

''(C) conduct mission engineering, architecting, and design of the Joint Cyber Warfighting Architecture system of systems, and any successor effort;

''(D) maintain a validated Joint Cyber Warfighting Architecture system of systems mission architecture, updated regularly to inform the current and future constituent programs of the Joint Cyber Warfighting Architecture, and the continuous delivery pipelines of such programs;

''(E) ensure that the Joint Cyber Warfighting Architecture component solution architectures align with and support the Joint Cyber Warfighting Architecture system of systems mission architecture;

''(F) support integration of mission-specific capabilities, including mission-specific data, analytics, defensive tools, offensive tools, and intelligence systems, acquired through non-Joint Cyber Warfighting Architecture programs; and

''(G) carry out any other responsibilities determined appropriate by the Secretary of Defense, including the acquisition of cyber operations capabilities beyond the Joint Cyber Warfighting Architecture.

''(3) APPORTIONMENT OF RESPONSIBILITIES.—The Commander shall apportion the responsibilities under paragraph (2) across the offices established pursuant to paragraph (1).

''(4) AUTHORITY.—The Secretary shall ensure that the offices established pursuant to paragraph (1) are empowered with the authority necessary to compel and enforce compliance with decisions and directives issued pursuant to the responsibilities under paragraph (2).

''(b) ARCHITECTURE COMPONENTS.—The Commander shall serve as the sole sponsor and requirements manager for the Joint Cyber Warfighting Architecture and the constituent programs of such architecture, as determined by the Commander.

''(c) ORGANIZATION OF PROGRAM EXECUTIVE OFFICE.—

''(1) HEAD.—

''(A) REPORTING.—The head of the program executive office established under subsection (a)(1)(A) shall report to the Command Acquisition Executive of the United States Cyber Command.

''(B) ADDITIONAL OVERSIGHT.—In addition to the oversight of the head of the program executive office provided by the Command Acquisition Executive under subparagraph (A), the Under Secretary of Defense for Acquisition and Sustainment, the Under Secretary of Defense for Research and Engineering, and the Principal Cyber Advisor of the Department of Defense shall provide oversight of the head.

''(2) RESPONSIBILITIES.—The head of the program executive office shall—

''(A) exercise central technical authority for the Joint Cyber Warfighting Architecture;

''(B) manage and provide oversight of the implementation and integration of the Architecture; and

''(C) provide direction to subordinate program offices, as determined appropriate by the Commander.

''(d) PERSONNEL.—

''(1) NECESSARY POSITIONS.—The Commander of the United States Cyber Command shall ensure that the program executive office or any subordinate program management office established pursuant to subsection (a)(1) includes in the staff of the respective office a chief architect, a systems engineer, and a chief talent officer to—

''(A) develop a mission-driven Joint Cyber Warfighting Architecture optimized for execution of missions of the United States Cyber Command;

''(B) ensure the office is properly and effectively staffed; and

''(C) advise the head of the office with respect to the execution of—

''(i) the central technical authority for the Joint Cyber Warfighting Architecture;

''(ii) the management of the implementation and integration of the Joint Cyber Warfighting Architecture; and

''(iii) technical direction provided to subordinates responsible for individual Joint Cyber Warfighting Architecture programs.

''(2) STAFFING.—

''(A) IN GENERAL.—The Secretary of Defense, in coordination with the Commander of the United States Cyber Command, shall ensure that the offices established pursuant to subsection (a)(1) are appropriately staffed with expert talent, including from the following organizations, as appropriate:

''(i) The headquarters staff of the United States Cyber Command, the Cyber National Mission Force, the Joint Force Headquarters-Cyber, and the Cyber Mission Force.

''(ii) The Capabilities Directorate of the National Security Agency.

''(iii) The military departments.

''(iv) The Cyber Capabilities Support Office of the Air Force.

''(v) The Defense Advanced Research Projects Agency.

''(vi) The Strategic Capabilities Office.

''(vii) Research laboratories of the military departments.

''(viii) The Defense Information Systems Agency.

''(B) TECHNICAL TALENT.—In addition to the requirement under subparagraph (A), to support the permanent staffing of the offices established pursuant to subsection (a)(1), the Commander of the United States Cyber Command shall ensure that the offices deliberately hire and use technical talent resident in the defense industrial base, commercial technology industry, federally funded research and development centers, university affiliated research centers, and the rest of the Federal Government.

''(e) BUDGET EXECUTION CONTROL.—The Secretary shall provide to the United States Cyber Command the resources necessary to support the program executive office established under subsection (a)(1)(A) and the Commander of the United States Cyber Command shall exercise budget execution control over component programs of the Joint Cyber Warfighting Architecture that are subject to the responsibilities assigned to the Commander by section 1507 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81; 10 U.S.C. 167b note).

''(f) CONSTELLATION PROGRAM.—The Director of the Defense Advanced Research Projects Agency and the head of the program executive office established under subsection (a)(1)(A) shall plan and carry out the Constellation program by entering into transactions under section 4021 of title 10, United States Code. In carrying out the preceding sentence, the Secretary shall establish an effective framework and pipeline system for maturing cyber operations-relevant technologies developed by the Agency, integrating the technologies into Joint Cyber Warfighting Architecture capabilities, and transitioning the technologies into operational use by the United States Cyber Command.

''(g) TRANSITION.—The Secretary of Defense, in coordination with the Commander of the United States Cyber Command, shall transition responsibilities for the management and execution of Joint Cyber Warfighting Architecture programs from the military departments to the offices established pursuant to subsection (a)(1) by the earlier of the following:

''(1) The date on which—

''(A) the offices are appropriately staffed and resourced; and

''(B) the Commander determines that the transition is appropriate.

''(2) The date that is five years after the date of the enactment of this Act [Dec. 23, 2022].

''(h) REVIEW.—Not later than one year after the date of the enactment of this Act, the Under Secretary of Defense for Acquisition and Sustainment and the Commander of the United States Cyber Command, in coordination with the Under Secretary of Defense for Research and Engineering, the Principal Cyber Advisor of the Department of Defense, the Secretaries of the military departments, the Director of the Defense Advanced Research Projects Agency, and the Director of the National Security Agency, shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] an integrated review of the Joint Cyber Warfighting Architecture and all other capabilities required for the execution of the missions of the United States Cyber Command to determine the following:

''(1) The extent to which capabilities of the United States Cyber Command and the National Security Agency should be joint, mutually available, integrated, or interoperable.

''(2) Whether each of the Joint Cyber Warfighting Architecture capabilities has been effectively designed and architected to enable each of the missions of the United States Cyber Command.

''(3) How the Joint Cyber Warfighting Architecture will support defense of the Department of Defense Information Network and its relation to existing datasets, sensors, tools, firewalls, and capabilities deployed at each echelon of the Department of Defense Information Network.

''(4) What data, capabilities, and technologies external to the current Joint Cyber Warfighting Architecture programs, as of the date of the review, should be acquired as part of the Joint Cyber Warfighting Architecture and under the control of the offices established pursuant to subsection (a)(1).

''(5) What mission-specific data, capabilities, and technologies external to the current Joint Cyber Warfighting Architecture programs should integrate with or be interoperable with the Joint Cyber Warfighting Architecture system of systems.

''(6) The organization and staffing of such offices, including—

''(A) whether the program executive office should be responsible for overseeing the acquisition of the cyber operations capabilities of the United States Cyber Command generally or the Joint Cyber Warfighting Architecture specifically;

''(B) what subordinate program management offices should be established under the program executive office;

''(C) whether the Joint Cyber Warfighting Architecture programs should be consolidated within a single program management office; and

''(D) which personnel should be appointed to such offices pursuant to subsection (d)(1).

''(7) The timeline for the execution of the transition under subsection (g).

''(8) The acquisition strategy of the Department for procuring the Joint Cyber Warfighting Architecture and related capabilities, including relevant enterprise strategic initiatives and contracting strategies.

''(9) The responsibilities of the United States Cyber Command J2, J3, J5, J6, J8, and J9 in acquiring, authorizing, and managing cyber capabilities.

''(10) The physical locations of the offices established pursuant to subsection (a)(1).

''(i) BRIEFING REQUIRED.—Not later than 540 days after the date of the enactment of this Act [Dec. 23, 2022], the Under Secretary of Defense for Acquisition and Sustainment and the Commander of the United States Cyber Command shall jointly provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the status of the implementation of this section.

''(j) REPEAL.—[Repealed section 1645 of Pub. L. 114–92, formerly set out as a note preceding section 4571 of this title.]

''(k) JOINT CYBER WARFIGHTING ARCHITECTURE DEFINED.—In this section, the term 'Joint Cyber Warfighting Architecture' means the range of joint cyber warfighting systems and capabilities that support the full spectrum of military cyber operations, as designated by the Commander of the United States Cyber Command, and includes any such successor effort.''

TOTAL FORCE GENERATION FOR THE CYBERSPACE OPERATIONS FORCES

Pub. L. 117–263, div. A, title XV, §1533, Dec. 23, 2022, 136 Stat. 2903, provided that:

''(a) STUDY.—

''(1) REQUIREMENT.—Not later than June 1, 2024, the Secretary of Defense shall complete a study on the responsibilities of the military services for organizing, training, and presenting the total force to United States Cyber Command.

''(2) ELEMENTS.—The study under paragraph (1) shall assess the following:

''(A) Which military services should man, train, equip, and organize the forces necessary to execute the functions and missions of the Cyber Mission Force and the Cyberspace Operations Forces for assignment, allocation, and apportionment to, or under the directive authority of, the United States Cyber Command.

''(B) The sufficiency of the military service accession and training model to provide forces to the Cyberspace Operations Forces and the sufficiency of the accessions and personnel resourcing of the supporting command and control staffs necessary as a component to the United States Cyber Command.

''(C) The organization of the Cyber Mission Forces and whether the total forces or elements of the forces function best as a collection of independent teams or through a different model.

''(D) How to correct chronic shortages of proficient personnel in key work roles.

''(E) The need for additional work roles or skills to enable effective infrastructure management and generate access to targets.

''(F) What unique or training-intensive expertise is required for each of the work roles identified in subparagraph (E) and whether native talents to master unique and training-intensive work roles can be identified and how personnel with those talents can be developed, retained, and employed across the active and reserve components.

''(G) The appropriate pay scales, rotation or force management policies, career paths and progression, expertise-based grading, talent management practices, and training for each of those work roles, given expected operational requirements.

''(H) Whether a single military service should be responsible for basic, intermediate, and advanced training for the Cyber Mission Force.

''(I) The level of training required before an individual should be assigned, allocated, or apportioned to the United States Cyber Command.

''(J) Whether or how the duties of the Director of the National Security Agency and the duties of the Commander of United States Cyber Command, resting with a single individual, enable each respective organization, and whether technical directors and intelligence experts of the National Security Agency should serve rotations in the Cyber Mission Force.

''(K) How nonmilitary personnel, such as civilian government employees, contracted experts, commercial partners, and domain or technology-specific experts in industry or the intelligence community can serve in, augment, or support Cyber Mission Force teams.

''(L) What work roles in the Cyberspace Operations Forces can only be filled by military personnel, which work roles can be filled by civilian employees or contractors, and which work roles should be filled partially or fully by civilians due to the need for longevity of service to achieve required skill levels or retention rates.

''(M) How specialized cyber experience, developed and maintained in the reserve component, can be more effectively leveraged to support the Cyberspace Operations Forces through innovative force generation models.

''(N) Whether the Department of Defense should create a separate service to perform the functions and missions currently performed by Cyber Mission Force units generated by multiple military services.

''(O) Whether the Department of Defense is maximizing partnerships with industry and other nontraditional sources of expertise and capacity in the areas of critical infrastructure protection and information sharing.

''(P) Whether the Defense Readiness Reporting System of the Department of Defense is sufficient to capture Cyber Mission Force readiness metrics.

''(3) CONSIDERATIONS.—The study required by paragraph (1) shall consider existing models for total force generation practices and programs, as well as nontraditional and creative alternatives.

''(b) RECOMMENDATIONS.—

''(1) IN GENERAL.—Not later than June 1, 2024, the Principal Cyber Advisor of the Department of Defense and the Commander of the United States Cyber Command shall submit to the Secretary of Defense one or more recommendations, respectively, as to the future total force generation model for both the Cyber Mission Force and the Cyberspace Operations Forces.

''(2) MATTERS ADDRESSED.—The recommendations under paragraph (1) shall address, at a minimum, each of the elements identified in subsection (a)(2).

''(c) ESTABLISHMENT OF A REVISED MODEL REQUIRED.—

''(1) IN GENERAL.—Not later than December 31, 2024, the Secretary of Defense shall establish a revised total force generation model for the Cyberspace Operations Forces.

''(2) ELEMENTS.—In establishing a revised total force generation model under paragraph (1), the Secretary shall explicitly determine the following:

''(A) Whether the Navy should no longer be responsible for developing and presenting forces to the United States Cyber Command as part of the Cyber Mission Force or Cyberspace Operations Forces, including recommendations for corresponding transfer of responsibilities and associated resources and personnel for the existing and future year programmed Cyberspace Operations Forces or Cyber Mission Force resources.

''(B) Whether a single military service should be responsible for organizing, training, and equipping the Cyberspace Operations Forces, or if different services should be responsible for different components of the Cyberspace Operations Forces.

''(C) Whether modification of United States Cyber Command enhanced budget control authorities are necessary to further improve total force generation for Cyberspace Operations Forces.

''(D) Implications of low service retention rates for critical roles within the Cyber Mission Force, and the mix of actions necessary to correct them, including multiple rotations in critical work roles, length of service commitments, repeat tours within the Cyber Mission Force, retention incentives across the entire Cyberspace Operations Forces, and best practices for generating the future force.

''(d) IMPLEMENTATION PLAN.—Not later than June 1, 2025, the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] an implementation plan for effecting the revised total force generation model required under subsection (c).

''(e) PROGRESS BRIEFING.—Not later than 90 days after the date of the enactment of this Act [Dec. 23, 2022], and not less frequently than once every 180 days there-

after until receipt of the plan required by subsection (d), the Secretary shall provide the congressional defense committees with a briefing on the progress made in carrying out this section.

''(f) ADDITIONAL CONSIDERATIONS.—The Secretary shall ensure that subsections (a) through (c) are carried out with consideration to matters relating to the following:

''(1) The cybersecurity service providers, local defenders, and information technology personnel who own, operate, and defend the information networks of the Department of Defense.

''(2) Equipping the Cyberspace Operations Forces to include infrastructure management.

''(3) Providing intelligence support to the Cyberspace Operations Forces.

''(4) The resources, including billets, needed to account for any recommended changes.''

CORRECTING CYBER MISSION FORCE READINESS SHORTFALLS

Pub. L. 117–263, div. A, title XV, § 1534, Dec. 23, 2022, 136 Stat. 2906, provided that:

''(a) PLAN AND BRIEFING REQUIRED.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2022], the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Secretaries of the military departments shall jointly—

''(1) develop a near-term plan to correct readiness shortfalls in the Cyber Mission Forces over the period covered by the most recent future-years defense program submitted to Congress under section 221 of title 10, United States Code;

''(2) develop recommendations for such legislative action as the Secretary of Defense, the Chairman, and the Secretaries of the military departments jointly consider appropriate to correct the readiness shortfalls described in paragraph (1); and

''(3) provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the plan under paragraph (1) and the recommendations under paragraph (2).

''(b) IMPLEMENTATION.—Not later than 30 days after the date of the briefing provided under paragraph (3) of subsection (a), the Secretary of Defense and the Chairman shall commence implementation of the aspects of the plan developed under paragraph (1) of such subsection that are not dependent upon legislative action.

''(c) MATTERS TO BE ADDRESSED.—In developing the plan under paragraph (1) of subsection (a), the Secretary of Defense, the Chairman, and the Secretaries of the military departments shall consider and explicitly address through analysis the following potential courses of action, singly and in combination, to increase the availability of personnel in key work roles:

''(1) Determining the correct number of personnel necessary to fill key work roles, including the proper force mix of civilian, military, and contractor personnel, and the means necessary to meet those requirements.

''(2) Employing civilians rather than military personnel in key work roles.

''(3) Expanding training capacity.

''(4) Modifying or creating new training models.

''(5) Maximizing use of compensation and incentive authorities, including increasing bonuses and special pays, and alternative compensation mechanisms.

''(6) Modifying career paths and service policies to permit consecutive assignments in key work roles without jeopardizing promotion opportunities.

''(7) Increasing service commitments following training commensurate with the value of the key work role training.

''(8) Standardizing compensation models across the services.

''(9) Requiring multiple rotations within the Cyber Mission Forces for key work roles.

''(10) Adopting and implementing what are known as 'rank in person' policies that enable civilian personnel to be promoted on the basis of skills and abilities demonstrated in a given position.

''(11) A review of departmental guidance and processes consistent with section 167b(d)(2)(A)(x) of title 10, United States Code, with respect to the authority of the Commander of United States Cyber Command to monitor the promotions of certain cyber operations forces and coordinate with the Secretaries regarding the assignment, retention, training, professional military education, and special and incentive pays of certain cyber operations forces, including—

''(A) the recruiting, retention, professional military education, and promotion of certain cyber operations personnel;

''(B) the sharing of personnel data between the military departments and the United States Cyber Command; and

''(C) structures, departmental guidance, and processes developed between the military departments and the United States Special Operations Command with respect to the authority of the Commander of the United States Special Operations Command described in section 167(e)(2)(J) of title 10, United States Code, that could be used as a model for the United States Cyber Command.

''(d) KEY WORK ROLES DEFINED.—In this section, the term 'key work roles' means work roles that consist of access development, tool development, and exploitation analysis.''

REVIEW OF DEFINITIONS ASSOCIATED WITH CYBERSPACE OPERATIONS FORCES

Pub. L. 117–263, div. A, title XV, § 1557, Dec. 23, 2022, 136 Stat. 2924, provided that:

''(a) REVIEW.—Not later than 120 days after the date of the enactment of this Act [Dec. 23, 2022], the Secretary of Defense, acting through the Principal Cyber Advisor of the Department of Defense and the Principal Cyber Advisors of the military departments, shall—

''(1) review—

''(A) the memorandum of the Secretary of Defense dated December 12, 2019, concerning the definition of the term 'Department of Defense Cyberspace Operations Forces (DoD COF)'; and

''(B) the responsibilities of the Commander of the United States Cyber Command as the Cyberspace Joint Force Provider and Cyberspace Joint Force Trainer, with respect to forces included and excluded from the Cyberspace Operations Forces; and

''(2) update such memorandum and, as appropriate, update such responsibilities.

''(b) ELEMENTS.—The review under subsection (a) shall include the following:

''(1) A comprehensive assessment of units and components of the Department of Defense conducting defensive cyberspace operations which are not currently included in the definition specified in paragraph (1)(A) of such subsection.

''(2) Consideration of options for participation in the Cyberspace Operations Forces by forces without regard to whether the forces are included in such definition, including options under which—

''(A) forces currently excluded from the Cyberspace Operations Forces because of such definition may access training, resources, and expertise of the Cyberspace Operations Forces;

''(B) the Commander of the United States Cyber Command may issue advisory tasking to forces that are not Cyberspace Operations Forces pursuant to such definition; and

''(C) forces that are not Cyberspace Operations Forces pursuant to such definition are subject to training standards established by the Commander as the Cyberspace Joint Force Trainer.''

ASSIGNMENT OF CERTAIN BUDGET CONTROL RESPONSIBILITIES TO COMMANDER OF UNITED STATES CYBER COMMAND

Pub. L. 117–81, div. A, title XV, § 1507, Dec. 27, 2021, 135 Stat. 2030, provided that:

''(a) ASSIGNMENT OF RESPONSIBILITIES.—

''(1) IN GENERAL.—The Commander of United States Cyber Command shall, subject to the authority, direction, and control of the Principal Cyber Advisor of the Department of Defense, be responsible for directly controlling and managing the planning, programming, budgeting, and execution of resources to train, equip, operate, and sustain the Cyber Mission Forces.

''(2) EFFECTIVE DATE AND APPLICABILITY.—Paragraph (1) shall take effect on the date of the enactment of this Act [Dec. 27, 2021] and apply—

''(A) on January 1, 2022, for controlling and managing budget execution; and

''(B) beginning with fiscal year 2024 and each fiscal year thereafter for directly controlling and managing the planning, programming, budgeting, and execution of resources.

''(b) ELEMENTS.—

''(1) IN GENERAL.—The responsibilities assigned to the Commander of United States Cyber Command pursuant to subsection (a)(1) shall include the following:

''(A) Preparation of a program objective memorandum and budget estimate submission for the resources required to train, equip, operate, and sustain the Cyber Mission Forces.

''(B) Preparation of budget materials pertaining to United States Cyber Command for inclusion in the budget justification materials that are submitted to Congress in support of the Department of Defense budget for a fiscal year (as submitted with the budget of the President for a fiscal year under section 1105(a) of title 31, United States Code) that is separate from any other military service or component of the Department.

''(2) RESPONSIBILITIES NOT DELEGATED.—The responsibilities assigned to the Commander of United States Cyber Command pursuant to subsection (a)(1) shall not include the following:

''(A) Military pay and allowances.

''(B) Funding for facility support that is provided by the military services.

''(c) IMPLEMENTATION PLAN.—

''(1) IN GENERAL.—Not later than the date that is 30 days after the date of the enactment of this Act, the Comptroller General of the Department of Defense and the Commander of United States Cyber Command, in coordination with Chief Information Officer of the Department, the Principal Cyber Advisor, the Under Secretary of Defense for Acquisition and Sustainment, Cost Assessment and Program Evaluation, and the Secretaries of the military departments, shall jointly develop an implementation plan for the transition of responsibilities assigned to the Commander of United States Cyber Command pursuant to subsection (a)(1).

''(2) ELEMENTS.—The implementation plan developed under paragraph (1) shall include the following:

''(A) A budgetary review to identify appropriate resources for transfer to the Commander of United States Cyber Command for carrying out responsibilities assigned pursuant to subsection (a)(1).

''(B) Definitions of appropriate roles and responsibilities.

''(C) Specification of all program elements and sub-elements, and the training, equipment, Joint Cyber Warfighting Architecture capabilities, other enabling capabilities and infrastructure, intelligence support, operations, and sustainment investments in each such program element and sub-element for which the Commander of United States Cyber Command is responsible.

''(D) Specification of all program elements and sub-elements, and the training, equipment, Joint Cyber Warfighting Architecture capabilities, other enabling capabilities and infrastructure, intelligence support, operations, and sustainment investments in each such program element and sub-element relevant to or that support the Cyber Mission Force for which the Secretaries of the military departments are responsible.

''(E) Required levels of civilian and military staffing within United States Cyber Command to carry out subsection (a)(1), and an estimate of when such levels of staffing will be achieved.

''(d) BRIEFING.—

''(1) IN GENERAL.—Not later than the earlier of the date on which the implementation plan under subsection (c) is developed or the date that is 90 days after the date of the enactment of this Act, the Secretary of Defense shall provide the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the implementation plan.

''(2) ELEMENTS.—The briefing required by paragraph (1) shall address any recommendations for when and how the Secretary of Defense should delegate to the Commander of United States Cyber Command budget authority for the Cyber Operations Forces (as such term is defined in the memorandum issued by the Secretary of Defense on December 12, 2019, relating to the definition of 'Department of Defense Cyberspace Operations Forces (DoD COF)'), after successful implementation of the responsibilities described in subsection (a) relating to the Cyber Mission Forces.''

Executive Documents

ELEVATION OF U.S. CYBER COMMAND TO A UNIFIED COMBATANT COMMAND

Memorandum of President of the United States, Aug. 15, 2017, 82 F.R. 39953, provided:

Memorandum for the Secretary of Defense

Pursuant to my authority as the Commander in Chief and under sections 161 and 167b of title 10, United States Code, and in consultation with the Secretary of Defense and the Chairman of the Joint Chiefs of Staff, I direct that U.S. Cyber Command be established as a Unified Combatant Command. I also direct the Secretary of Defense to recommend an officer for my nomination and Senate confirmation as commander in order to establish U.S. Cyber Command as a Unified Combatant Command.

I assign to U.S. Cyber Command: (1) all the general responsibilities of a Unified Combatant Command; (2) the cyberspace-related responsibilities previously assigned to the Commander, U.S. Strategic Command; (3) the responsibilities of Joint Force Provider and Joint Force Trainer; and (4) all other responsibilities identified in section 167b of title 10, United States Code. The comprehensive list of authorities and responsibilities for U.S. Cyber Command will be included in the next update to the Unified Command Plan.

I further direct that the Secretary of Defense, in coordination with the Director of National Intelligence, provide a recommendation and, as appropriate, a plan to me regarding the future command relationship between the U.S. Cyber Command and the National Security Agency.

Consistent with section 161(b)(2) of title 10, United States Code, and section 301 of title 3, United States Code, you are directed to notify the Congress on my behalf.

You are authorized and directed to publish this memorandum in the Federal Register.

DONALD J. TRUMP.

[§ 168. Repealed. Pub. L. 114–328, div. A, title XII, § 1253(a)(1)(A), Dec. 23, 2016, 130 Stat. 2532]

Section, added Pub. L. 103–337, div. A, title XIII, § 1316(a)(1), Oct. 5, 1994, 108 Stat. 2898; amended Pub. L. 104–106, div. A, title IV, § 416, Feb. 10, 1996, 110 Stat. 289; Pub. L. 108–375, div. A, title IV, § 416(e), Oct. 28, 2004, 118 Stat. 1868; Pub. L. 110–181, div. A, title XII, § 1201, Jan. 28, 2008, 122 Stat. 363; Pub. L. 110–417, [div. A], title XII, § 1202(a), Oct. 14, 2008, 122 Stat. 4622, related to military-to-military contacts and comparable activities.