2018—Subsec. (c)(1). Pub. L. 115–232 substituted ''Sections 246, 251, 252, 253, 321,'' for ''Sections 311, 321, 331, 332, 333,''.

2016—Subsec. (a). Pub. L. 114–328, §1251(b)(6), which directed striking out ''under the authorities in subsection (c)'' after ''submitted'', was executed by striking out ''under the authorities specified in subsection (c)'' after ''submitted'', to reflect the probable intent of Congress.

Pub. L. 114–328, §1251(b)(1)–(5), in heading, substituted ''Annual Report Required'' for ''Biennial Report Required'', and, in text, substituted ''Not later than January 31 of each year beginning in 2018, the Secretary of Defense'' for ''Not later than February 1 of each of 2016, 2018, and 2020, the Secretary of Defense'', ''appropriate congressional committees'' for ''congressional defense committees'', ''assistance'' for ''security assistance'', and ''the fiscal year'' for ''the two fiscal years'' and inserted ''under the authorities in subsection (c)'' after ''Department of Defense''.

Subsec. (b)(1). Pub. L. 114–328, §1251(c)(1), inserted '', duration,'' after ''purpose''.

Subsec. (b)(2). Pub. L. 114–328, §1251(c)(2), substituted ''The cost and expenditures'' for ''The cost''.

Subsec. (b)(4) to (6). Pub. L. 114–328, §1251(c)(3), added pars. (4) to (6).

Subsec. (c)(1). Pub. L. 114–328, §1246(d)(2)(A), which directed amendment of subsec. (c)(1) by inserting ''341,'' after ''333,'', was executed by making the insertion after ''321,'' to reflect the probable intent of Congress and the intervening amendment by Pub. L. 115–232. See 2018 Amendment note above.

Pub. L. 114–328, §1251(d)(1), added par. (1) and struck out former par. (1) which read as follows: ''Section 127d of title 10, United States Code, relating to authority to provide logistic support, supplies, and services to allied forces participating in a combined operation with the Armed Forces.''

Subsec. (c)(2), (3). Pub. L. 114–328, §1251(d)(6), substituted ''of this title'' for ''of title 10, United States Code''.

Subsec. (c)(4). Pub. L. 114–328, §1251(d)(2), (3), (6), redesignated par. (6) as (4), substituted ''of this title'' for ''of title 10, United States Code'', and struck out former par. (4) which read as follows: ''Section 2010 of title 10, United States Code, relating to authority to reimburse foreign troops for participation in combined exercises.''

Subsec. (c)(5). Pub. L. 114–328, §1251(d)(2), (3), (6), redesignated par. (8) as (5), substituted ''of this title'' for ''of title 10, United States Code'', and struck out former par. (5) which read as follows: ''Section 2011 of title 10, United States Code, relating to authority to reimburse foreign troops for participation in Joint Combined Exercise Training.''

Subsec. (c)(6). Pub. L. 114–328, §1251(d)(3), redesignated par. (9) as (6). Former par. (6) redesignated (4).

Subsec. (c)(7). Pub. L. 114–328, §1251(d)(2), (3), redesignated par. (13) as (7) and struck out former par. (7) which read as follows: ''Section 2282 of title 10, United States Code (as added by section 1205 of this Act), relating to authority to build the capacity of foreign military forces, or the predecessor authority to such section in section 1206 of the National Defense Authorization Act for Fiscal Year 2006 (Public Law 109–163; 119 Stat. 3456).''

Subsec. (c)(8), (9). Pub. L. 114–328, §1251(d)(3), redesignated pars. (14) and (15) as (8) and (9), respectively. Former pars. (8) and (9) redesignated (5) and (6), respectively.

Subsec. (c)(10). Pub. L. 114–328, §1251(d)(2), (3), redesignated par. (16) as (10) and struck out former par. (10) which read as follows: ''Section 1205 of the National Defense Authorization Act for Fiscal Year 2014 (32 U.S.C. 107 note), relating to authority for National Guard State Partnership program.''

Subsec. (c)(11), (12). Pub. L. 114–328, §1251(d)(2), (4), added pars. (11) and (12) and struck out former pars. (11) and (12) which read as follows:

''(11) Section 1081 of the National Defense Authorization Act for Fiscal Year 2012 (10 U.S.C. 168 note), relating to the Ministry of Defense Advisors program.

''(12) Section 1207 of the National Defense Authorization Act for Fiscal Year 2012 (22 U.S.C. 2151 note), relating to the Global Security Contingency Fund.''

Subsec. (c)(13). Pub. L. 114–328, §1251(d)(5), redesignated par. (17) as (13). Former par. (13) redesignated (7).

Subsec. (c)(14) to (16). Pub. L. 114–328, §1251(d)(3), redesignated pars. (14) to (16) as (8) to (10), respectively.

Subsec. (c)(17). Pub. L. 114–328, §1251(d)(5), redesignated par. (17) as (13).

Subsec. (d). Pub. L. 114–328, §1251(e), designated existing provisions as par. (1) and inserted heading, substituted ''Except as provided in paragraph (2), if any information'' for ''If any information'', and added par. (2).

Subsec. (e). Pub. L. 114–328, §1251(f), inserted ''that may also include other sensitive information'' after ''annex''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2016 AMENDMENT

Pub. L. 114–328, div. A, title XII, §1246(d)(2), Dec. 23, 2016, 130 Stat. 2521, provided that the amendment made by section 1246(d)(2)(A) is effective as of January 1, 2020.

APPLICABILITY OF AMENDMENT TO ANNUAL REPORT REQUIREMENTS

Pub. L. 117–263, div. A, title XII, §1202(e), Dec. 23, 2022, 136 Stat. 2826, provided that: ''With respect to a report that was required to be submitted under section 386 of title 10, United States Code, prior to the date of the enactment of this Act [Dec. 23, 2022], that has not been submitted as of such date and relates to a year preceding fiscal year 2023, such a report may be submitted in accordance with—

''(1) the requirements of such section 386 as amended by subsection (d); or

''(2) the requirements of such section 386 as in effect on the day before the date of the enactment of this Act.''

CHAPTER 19—CYBER AND INFORMATION OPERATIONS MATTERS

Editorial Notes

AMENDMENTS

2023—Pub. L. 118–31, div. A, title XV, §§1501(1), 1502(a)(1), title XVIII, §1801(a)(6), Dec. 22, 2023, 137 Stat. 533, 683, added item 391b and made identical amendments redesignating item 398 ''Pilot program for shar-

ing cyber capabilities and related information with foreign operational partners'' as 398a. Amendments were made pursuant to operation of section 102 of this title.

2022—Pub. L. 117–263, div. A, title X, §1052(b), title XV, §§1501(b)(1), 1502(a), 1521, 1551(b), Dec. 23, 2022, 136 Stat. 2777, 2877, 2879, 2897, 2919, added items 391a, 392a, and 399 and two items 398.

2019—Pub. L. 116–92, div. A, title XVI, §1631(a)(2)(A), Dec. 20, 2019, 133 Stat. 1742, substituted ''CYBER AND INFORMATION OPERATIONS MATTERS'' for ''CYBER MATTERS'' in chapter heading and added item 397.

2018—Pub. L. 115–232, div. A, title XVI, §1631(c)(2), Aug. 13, 2018, 132 Stat. 2123, added items 394 to 396.

2015—Pub. L. 114–92, div. A, title X, §1081(a)(4), title XVI, §1641(c)(2), Nov. 25, 2015, 129 Stat. 1001, 1116, substituted ''Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors'' for ''Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors'' in item 391 and added item 393.

2014—Pub. L. 113–291, div. A, title XVI, §1633(d), Dec. 19, 2014, 128 Stat. 3643, added item 392.

Statutory Notes and Related Subsidiaries

ESTABLISHMENT OF THE DEPARTMENT OF DEFENSE HACKATHON PROGRAM

Pub. L. 118–159, div. A, title XV, §1503, Dec. 23, 2024, 138 Stat. 2132, provided that:

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2024], the Chief Digital and Artificial Intelligence Officer of the Department of Defense, in coordination with the Chairman of the Joint Chiefs of Staff and the Chief Information Officer of the Department of Defense, shall establish a program (to be known as the 'Department of Defense Hackathon Program') under which the commanders of combatant commands and the Secretaries of the military departments shall carry out not fewer than four Hackathons each year.

''(b) PROGRAM MANAGEMENT.—The Chief Digital and Artificial Intelligence Officer of the Department of Defense shall develop and implement standards for carrying out Hackathons, provide supporting technical infrastructure to the host of each Hackathon, and determine the hosts each year under subsection (c)(1).

''(c) HOSTS.—

''(1)(A) Each year, two commanders of combatant commands shall each carry out a Hackathon and two Secretaries of military departments shall each carry out a Hackathon, as determined by the Chief Digital and Artificial Intelligence Officer of the Department of Defense in accordance with this subsection.

''(B) The commanders of combatant commands and the Secretaries of military departments carrying out Hackathons pursuant to subparagraph (A) shall change each year.

''(C) Each host of a Hackathon shall—

''(i) provide to the participants invited to participate in such Hackathon a per diem allowance in accordance with section 5702 of title 5, United States Code, or section 452 of title 37, United States Code, as applicable; and

''(ii) not later than 60 days after the completion of such Hackathon, make available to the Department of Defense a report on such Hackathon.

''(2) Any commander of a combatant command or Secretary of a military department may carry out a Hackathon in addition to the Hackathons required under paragraph (1).

''(d) HACKATHON OBJECTIVES.—

''(1) The host of each Hackathon shall establish objectives for the Hackathon that address a critical, technical challenge of the combatant command or military department of the host, as applicable, through the use of individuals with specialized and relevant skills, including data scientists, developers, software engineers, and other specialists as determined appropriate by the Chief Digital and Artificial Intelligence Officer of the Department of Defense or the host.

''(2) In addition to the objectives established by the host of a Hackathon under paragraph (1), the objectives for each Hackathon shall include—

''(A) fostering innovation across the Department of Defense, including in military departments and the combatant commands; and

''(B) creating repeatable processes enabling the commanders of combatant commands and the Secretaries of the military departments to more rapidly identify and develop solutions to critical, technical challenges across the Department of Defense.

''(e) DEFINITIONS.—In this section—

''(1) the term 'Hackathon' means an event carried out under the Program at which employees across the Department of Defense meet to collaboratively attempt to develop functional software or hardware solutions during the event to solve a critical, technical challenge determined by the host;

''(2) the term 'host', with respect to a Hackathon, means the commander of the combatant command or the Secretary of the military department carrying out the Hackathon;

''(3) the term 'military department' has the meaning given such term in section 101(a) of title 10, United States Code; and

''(4) the term 'Program' means the program established under subsection (a).''

ALIGNMENT OF DEPARTMENT OF DEFENSE CYBER INTERNATIONAL STRATEGY WITH NATIONAL DEFENSE STRATEGY AND DEPARTMENT OF DEFENSE CYBER STRATEGY

Pub. L. 117–263, div. A, title XV, §1506, Dec. 23, 2022, 136 Stat. 2882, provided that:

''(a) ALIGNMENT REQUIRED.—Not later than 270 days after the date of the enactment of this Act [Dec. 23, 2022], the Secretary of Defense, acting through the Under Secretary of Defense for Policy and in coordination with the commanders of the combatant commands and the Director of the Joint Staff, shall undertake efforts to align the cybersecurity cooperation enterprise of the Department of Defense and the cyberspace operational partnerships of the Department with—

''(1) the national defense strategy published in 2022 pursuant to section 113(g) of title 10, United States Code;

''(2) the Cyber Strategy of the Department published during fiscal year 2023; and

''(3) the current International Cyberspace Security Cooperation Guidance of the Department, as of the date of the enactment of this Act.

''(b) ELEMENTS.—The alignment efforts under subsection (a) shall include the following efforts within the Department of Defense:

''(1) Efforts to build the internal capacity of the Department to support international strategy policy engagements with allies and partners of the United States.

''(2) Efforts to coordinate and align cyberspace operations with foreign partners of the United States, including alignment between hunt-forward missions and other cyber international strategy activities conducted by the Department, including identification of processes, working groups, and methods to facilitate coordination between geographic combatant commands and the United States Cyber Command.

''(3) Efforts to deliberately cultivate operational and intelligence-sharing partnerships with key allies and partners of the United States to advance the cyberspace operations objectives of the Department.

''(4) Efforts to identify key allied and partner networks, infrastructure, and systems that the Joint Force will rely upon for warfighting and to—

''(A) support the cybersecurity and cyber defense of those networks, infrastructure, and systems;

''(B) build partner capacity to actively defend those networks, infrastructure, and systems;

''(C) eradicate malicious cyber activity that has compromised those networks, infrastructure, and systems, such as when identified through hunt-forward operations; and

''(D) leverage the commercial and military cybersecurity technology and services of the United States to harden and defend those networks, infrastructure, and systems.

''(5) Efforts to secure the environments and networks of mission partners of the United States used to hold intelligence and information originated by the United States.

''(6) Prioritization schemas, funding requirements, and efficacy metrics to drive cyberspace security investments in the tools, technologies, and capacity-building efforts that will have the greatest positive impact on the resilience and ability of the Department to execute its operational plans and achieve integrated deterrence.

''(c) ORGANIZATION.—The Under Secretary of Defense for Policy shall lead efforts to implement this section. In doing so, the Under Secretary shall consult with the Secretary of State, the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the Director of the Federal Bureau of Investigation, to align plans and programs as appropriate.

''(d) ANNUAL BRIEFINGS.—

''(1) REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act, and not less frequently than once each fiscal year until September 30, 2025, the Under Secretary of Defense for Policy shall provide to the Committees on Armed Services of the Senate and the House of Representatives a briefing on the implementation of this section.

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

''(A) An overview of efforts undertaken pursuant to this section.

''(B) An accounting of all the security cooperation activities of the Department germane to cyberspace and changes made pursuant to implementation of this section.

''(C) A detailed schedule with target milestones and required expenditures for all planned activities related to the efforts described in subsection (b).

''(D) Interim and final metrics for building the cyberspace security cooperation enterprise of the Department.

''(E) Identification of such additional funding, authorities, and policies, as the Under Secretary determines may be required.

''(F) Such recommendations as the Under Secretary may have for legislative action to improve the effectiveness of cyberspace security cooperation of the Department with foreign partners and allies.

''(e) ANNUAL REPORT.—Not later than 90 days after the date of the enactment of this Act and not less frequently than once each year thereafter until January 1, 2025, the Under Secretary of Defense for Policy shall submit to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives a report summarizing the cyber international strategy activities of the Department, including within the cybersecurity cooperation enterprise of the Department and the cyber operational partnerships of the Department.''

ENHANCEMENT OF CYBERSPACE TRAINING AND SECURITY COOPERATION

Pub. L. 117–263, div. A, title XV, § 1507, Dec. 23, 2022, 136 Stat. 2883, provided that:

''(a) ENHANCED TRAINING.—

''(1) REQUIREMENT.—The Under Secretary of Defense for Intelligence and Security and the Under Secretary of Defense for Policy, in coordination with the Commander of United States Cyber Command, the Director of the Defense Security Cooperation Agency, and the Director of the Defense Intelligence Agency, shall develop enhanced guidance for and implement training on cyberspace security cooperation at the Defense Security Cooperation University and the Joint Military Attaché School.

''(2) TIMING.—The Under Secretaries shall develop the enhanced guidance and implement the training under paragraph (1)—

''(A) by not later than one year after the date of the enactment of this Act [Dec. 23, 2022] with respect to the Joint Military Attaché School; and

''(B) by not later than September 30, 2025, with respect to the Defense Security Cooperation University.

''(3) ELEMENTS.—The Under Secretaries shall ensure that the training on cyberspace security cooperation under paragraph (1)—

''(A) is tailored to the trainees' anticipated embassy role and functions; and

''(B) provides familiarity with—

''(i) the different purposes of cyberspace engagements with partners and allies of the United States, including threat awareness, cybersecurity, mission assurance, and operations;

''(ii) the types of cyberspace security cooperation programs and activities available for partners and allies of the United States, including bilateral and multilateral cyberspace engagements, information and intelligence sharing, training, and exercises;

''(iii) the United States Cyber Command cyberspace operations with partners, including an overview of the Hunt Forward mission and process;

''(iv) the roles and responsibilities of the United States Cyber Command, the geographic combatant commands, and the Defense Security Cooperation Agency for cybersecurity cooperation within the Department of Defense; and

''(v) such other matters as the Under Secretaries, in coordination with the Commander of United States Cyber Command, consider appropriate.

''(4) REQUIREMENTS.—The baseline familiarization training developed under subsection (a) shall be a required element for all participants in the Defense Security Cooperation University, the Attaché Training Program, and the Attaché Staff Training Program of the Joint Military Attaché School.

''(b) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Under Secretary of Defense for Intelligence and Security and the Under Secretary of Defense for Policy, in coordination with the Commander of the United States Cyber Command, the Director of the Defense Security Cooperation Agency, and the Director of the Defense Intelligence Agency, shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report on the requirements and considerations to implement enhanced training and coordination to advance cyberspace security cooperation with foreign partners. The study may consider such areas as the following:

''(1) Sufficiency of the training provided in the Defense Security Cooperation University and the Joint Military Attaché School.

''(2) Additional training requirements, familiarization requirements, or both such requirements necessary for officers assigned to particular locations or positions.

''(3) Areas for increased cooperation.

''(4) A plan for completing the activities required by subsection (a).

''(5) Additional resources required to complete such activities.

''(c) BRIEFING.—Not later than 30 days after the date on which the Under Secretary of Defense for Intelligence and Security and the Under Secretary of Defense for Policy submit the report under subsection (b), the Under Secretaries, in coordination with the Commander of the United States Cyber Command, the Director of the Defense Security Cooperation Agency, and the Director of the Defense Intelligence Agency, shall

provide to the Committees on Armed Services of the Senate and the House of Representatives a briefing on the findings from the report on enhancing training and coordination to advance cyberspace security cooperation described in such subsection. Such briefing shall include a discussion on the enhanced training meeting the elements under subsection (a)(3) and a plan for future updates and sustainment of such training.''

§ 391. Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors

(a) DESIGNATION OF DEPARTMENT COMPONENT TO RECEIVE REPORTS.—The Secretary of Defense shall designate a component of the Department of Defense to receive reports of cyber incidents from contractors in accordance with this section and section 393 of this title or from other governmental entities.

(b) PROCEDURES FOR REPORTING CYBER INCIDENTS.—The Secretary of Defense shall establish procedures that require an operationally critical contractor to report in a timely manner to component designated under subsection (a) each time a cyber incident occurs with respect to a network or information system of such operationally critical contractor.

(c) PROCEDURE REQUIREMENTS.—

(1) DESIGNATION AND NOTIFICATION.—The procedures established pursuant to subsection (a) shall include a process for—

(A) designating operationally critical contractors; and

(B) notifying a contractor that it has been designated as an operationally critical contractor.

(2) RAPID REPORTING.—The procedures established pursuant to subsection (a) shall require each operationally critical contractor to rapidly report to the component of the Department designated pursuant to subsection (d)(2)(A) on each cyber incident with respect to any network or information systems of such contractor. Each such report shall include the following:

(A) An assessment by the contractor of the effect of the cyber incident on the ability of the contractor to meet the contractual requirements of the Department.

(B) The technique or method used in such cyber incident.

(C) A sample of any malicious software, if discovered and isolated by the contractor, involved in such cyber incident.

(D) A summary of information compromised by such cyber incident.

(3) DEPARTMENT ASSISTANCE AND ACCESS TO EQUIPMENT AND INFORMATION BY DEPARTMENT PERSONNEL.—The procedures established pursuant to subsection (a) shall—

(A) include mechanisms for Department personnel to, if requested, assist operationally critical contractors in detecting and mitigating penetrations; and

(B) provide that an operationally critical contractor is only required to provide access to equipment or information as described in subparagraph (A) to determine whether information created by or for the Department in connection with any Department program was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated.

(4) PROTECTION OF TRADE SECRETS AND OTHER INFORMATION.—The procedures established pursuant to subsection (a) shall provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person.

(5) DISSEMINATION OF INFORMATION.—The procedures established pursuant to subsection (a) shall limit the dissemination of information obtained or derived through the procedures to entities—

(A) with missions that may be affected by such information;

(B) that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(C) that conduct counterintelligence or law enforcement investigations; or

(D) for national security purposes, including cyber situational awareness and defense purposes.

(d) PROTECTION FROM LIABILITY OF OPERATIONALLY CRITICAL CONTRACTORS.—(1) No cause of action shall lie or be maintained in any court against any operationally critical contractor, and such action shall be promptly dismissed, for compliance with this section and contract requirements established pursuant to Defense Federal Acquisition Regulation Supplement clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, that is conducted in accordance with procedures established pursuant to subsection (b) and such contract requirements.

(2)(A) Nothing in this section shall be construed—

(i) to require dismissal of a cause of action against an operationally critical contractor that has engaged in willful misconduct in the course of complying with the procedures established pursuant to subsection (b); or

(ii) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

(B) In any action claiming that paragraph (1) does not apply due to willful misconduct described in subparagraph (A), the plaintiff shall have the burden of proving by clear and convincing evidence the willful misconduct by each operationally critical contractor subject to such claim and that such willful misconduct proximately caused injury to the plaintiff.

(C) In this subsection, the term ''willful misconduct'' means an act or omission that is taken—

(i) intentionally to achieve a wrongful purpose;

(ii) knowingly without legal or factual justification; and

(iii) in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit.

(e) DEFINITIONS.—In this section:

(1) CYBER INCIDENT.—The term ''cyber incident'' means actions taken through the use of

computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

(2) OPERATIONALLY CRITICAL CONTRACTOR.—The term ''operationally critical contractor'' means a contractor designated by the Secretary for purposes of this section as a critical source of supply for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

(Added Pub. L. 113–291, div. A, title XVI, §1632(a), Dec. 19, 2014, 128 Stat. 3639; amended Pub. L. 114–92, div. A, title XVI, §1641(b), (c)(1), Nov. 25, 2015, 129 Stat. 1115, 1116; Pub. L. 116–283, div. A, title XVII, §1704, Jan. 1, 2021, 134 Stat. 4082.)

Editorial Notes

AMENDMENTS

2021—Subsec. (d)(1). Pub. L. 116–283 inserted ''and contract requirements established pursuant to Defense Federal Acquisition Regulation Supplement clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting,'' after ''compliance with this section'' and ''and such contract requirements'' before period at end.

2015—Subsec. (a). Pub. L. 114–92, §1641(c)(1), substituted ''and section 393 of this title'' for ''and with section 941 of the National Defense Authorization Act for Fiscal Year 2013 (10 U.S.C. 2224 note)''.

Subsecs. (d), (e). Pub. L. 114–92, §1641(b), added subsec. (d) and redesignated former subsec. (d) as (e).

Statutory Notes and Related Subsidiaries

SENIOR MILITARY ADVISOR FOR CYBER POLICY AND DEPUTY PRINCIPAL CYBER ADVISOR

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, which authorized the Secretary of Defense to designate an officer within the Office of the Under Secretary of Defense for Policy to serve within that Office as Senior Military Advisor for Cyber Policy, and concurrently, as Deputy Principal Cyber Advisor, was transferred to section 392a of this chapter and designated as subsec. (b) of that section by Pub. L. 117–263, div. A, title XV, §1501(b)(3)(A), Dec. 23, 2022, 136 Stat. 2878.

CYBER GOVERNANCE STRUCTURES AND PRINCIPAL CYBER ADVISORS ON MILITARY CYBER FORCE MATTERS

Pub. L. 116–92, div. A, title XVI, §1657, Dec. 20, 2019, 133 Stat. 1767, which authorized each of the secretaries of the military departments, in consultation with the service chiefs, to 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, was transferred to section 392a of this chapter and designated as subsec. (c) of that section by Pub. L. 117–263, div. A, title XV, §1501(b)(4)(A), Dec. 23, 2022, 136 Stat. 2878.

CONSORTIA OF UNIVERSITIES TO ADVISE SECRETARY OF DEFENSE ON CYBERSECURITY MATTERS

Pub. L. 116–92, div. A, title XVI, §1659, Dec. 20, 2019, 133 Stat. 1770, as amended by Pub. L. 117–81, div. A, title XV, §1530, Dec. 27, 2021, 135 Stat. 2049; Pub. L. 117–263, div. A, title XV, §1505, Dec. 23, 2022, 136 Stat. 2881; Pub. L. 118–31, div. A, title XV, §1531(c)(3), Dec. 22, 2023, 137 Stat. 562, provided that:

''(a) ESTABLISHMENT AND FUNCTION.—The Secretary of Defense shall establish a consortium of universities to assist the Secretary on cybersecurity matters relating to the following:

''(1) To provide the Secretary a formal mechanism to communicate with consortium members regarding the Department of Defense's cybersecurity strategic plans, cybersecurity requirements, and priorities for basic and applied cybersecurity research.

''(2) To advise the Secretary on the needs of academic institutions related to cybersecurity and research conducted on behalf of the Department and provide feedback to the Secretary from members of the consortium or consortia.

''(3) To serve as a focal point or focal points for the Secretary and the Department for the academic community on matters related to cybersecurity, cybersecurity research, conceptual and academic developments in cybersecurity, and opportunities for closer collaboration between academia and the Department.

''(4) To provide to the Secretary access to the expertise of the institutions of the consortium or consortia on matters relating to cybersecurity.

''(5) To align the efforts of such members in support of the Department.

''(b) MEMBERSHIP.—The consortium established under subsection (a) shall be open to all universities that have been designated as centers of academic excellence by the Director of the National Security Agency or the Secretary of Homeland Security.

''(c) ORGANIZATION.—

''(1) DESIGNATION OF ADMINISTRATIVE CHAIR.—The Secretary of Defense shall designate the National Defense University College of Information and Cyberspace to function as the administrative chair of the consortium established pursuant to subsection (a).

''(2) DUTIES OF ADMINISTRATIVE CHAIR.—The administrative chair designated under paragraph (1) for the consortium shall—

''(A) act as the leader of the consortium;

''(B) be the liaison between the consortium and the Secretary;

''(C) distribute requests from the Secretary for advice and assistance to appropriate members of the consortium and coordinate responses back to the Secretary; and

''(D) act as a clearinghouse for Department of Defense requests relating to assistance on matters relating to cybersecurity and to provide feedback to the Secretary from members of the consortium.

''(3) EXECUTIVE COMMITTEE.—The Secretary, in consultation with the administrative chair, may form an executive committee for the consortium that is comprised of representatives of the Federal Government to assist the chair with the management and functions of the consortium.

''(d) CONSULTATION.—The Secretary shall meet with such members of the consortium as the Secretary considers appropriate, not less frequently than twice each year or at such periodicity as is agreed to by the Secretary and the consortium.

''(e) PROCEDURES.—The Secretary shall establish procedures for organizations within the Department to access the work product produced by and the research, capabilities, and expertise of a consortium established under subsection (a) and the universities that constitute such consortium.

''(f) SUPPORT CENTER.—

''(1) ESTABLISHMENT.—The Secretary shall establish a center to provide support to the consortium established under subsection (a).

''(2) COMPOSITION.—

''(A) REQUIREMENT.—The center established under paragraph (1) shall be composed of one or two universities, as the Secretary considers appropriate, that—

''(i) have been designated as centers of academic excellence by the Director of the National Security Agency or the Secretary of Homeland Security; and

''(ii) are eligible for access to classified information.

''(B) PUBLICATION.—The Secretary shall publish in the Federal Register the process for selection of universities to serve as the center established under paragraph (1).

''(3) FUNCTIONS.—The functions of the center established under paragraph (1) are as follows:

''(A) To promote the consortium established under subsection (a).

''(B) To distribute on behalf of the Department requests for information or assistance to members of the consortium.

''(C) To collect and assemble responses from requests distributed under subparagraph (B).

''(D) To provide additional administrative support for the consortium.

''(g) DISCHARGE THROUGH DIRECTOR.—In carrying out this section, the Secretary of Defense shall act through the Director of the office established under section 2192c of title 10, United States Code.''

ISSUANCE OF PROCEDURES

Pub. L. 113–291, div. A, title XVI, §1632(b), Dec. 19, 2014, 128 Stat. 3640, provided that: ''The Secretary shall establish the procedures required by subsection (b) of section 391 of title 10, United States Code, as added by subsection (a) of this section, not later than 90 days after the date of the enactment of this Act [Dec. 19, 2014].''

ASSESSMENT OF DEPARTMENT POLICIES

Pub. L. 113–291, div. A, title XVI, §1632(c), Dec. 19, 2014, 128 Stat. 3640, provided that:

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of the Act [Dec. 19, 2014], the Secretary of Defense shall complete an assessment of—

''(A) requirements that were in effect on the day before the date of the enactment of this Act for contractors to share information with Department components regarding cyber incidents (as defined in subsection (d) [now (e)] of such section 391 [10 U.S.C. 391(e)]) with respect to networks or information systems of contractors; and

''(B) Department policies and systems for sharing information on cyber incidents with respect to networks or information systems of Department contractors.

''(2) ACTIONS FOLLOWING ASSESSMENT.—Upon completion of the assessment required by paragraph (1), the Secretary shall—

''(A) designate a Department component under subsection (a) of such section 391; and

''(B) issue or revise guidance applicable to Department components that ensures the rapid sharing by the component designated pursuant to such section 391 or section 941 of the National Defense Authorization Act for Fiscal Year 2013 [Pub. L. 112–239] (10 U.S.C. 2224 note) of information relating to cyber incidents with respect to networks or information systems of contractors with other appropriate Department components.''

§ 391a. Annual reports on support by military departments for United States Cyber Command

(a) REPORTS.—Not later than 15 days after the date on which the Secretary of Defense submits to Congress the defense budget materials (as defined in section 239 of this title) for a fiscal year, the Commander of the United States Cyber Command shall submit to the congressional defense committees a report containing the following:

(1) An evaluation of whether each military department is meeting the requirements established by the Commander and validated by the Office of the Secretary of Defense, and is effectively implementing the plan required by section 1534 of the National Defense Authorization Act for Fiscal Year 2023, and the requirements established pursuant to section 1533 of such Act.

(2) For each military department evaluated under paragraph (1)—

(A) a certification that the military department is meeting such requirements; or

(B) a detailed explanation regarding how the military department is not meeting such requirements.

(b) ELEMENTS OF EVALUATION.—Each evaluation under subsection (a)(1) shall include, with respect to the military department being evaluated, the following:

(1) The adequacy of the policies, procedures, and execution of manning, training, and equipping personnel for employment within the Cyber Mission Force.

(2) The sufficiency and robustness of training curricula for personnel to be assigned to either the Cyber Mission Force or units within the cyberspace operations forces, and the compliance by the military department with training standards.

(3) The adequacy of the policies and procedures relating to the assignment and assignment length of members of the Army, Navy, Air Force, Marine Corps, or Space Force to the Cyber Mission Force.

(4) The efficacy of the military department in filling key work roles within the Cyber Mission Force, including the proper force mix of civilian, military, and contractor personnel, and the means necessary to meet requirements established by the Commander and validated by the Secretary of Defense.

(5) The adequacy of the investment to advance cyber-peculiar science and technology, particularly with respect to capability development for the Cyber Mission Force.

(6) The sufficiency of the policies, procedures, and investments relating to the establishment and management of military occupational specialty, designator, rating, or Air Force specialty code for personnel responsible for cyberspace operations, including an assessment of the effectiveness of the combination of policies determining availability and retention of sufficient numbers of proficient personnel in key work roles, including length of service commitment, the use of bonuses and special pays, alternative compensation mechanisms, and consecutive tours in preferred assignments.

(7) In coordination with the Principal Cyber Advisor of the Department of Defense, an evaluation of the use by the military department of the shared lexicon of the Department of Defense specific to cyberspace activities.

(8) The readiness of personnel serving in the Cyber Mission Force and the cyberspace operations forces to accomplish assigned missions.

(9) The adequacy of actions taken during the period of evaluation by the military department to respond to findings from any previous years' evaluations.

(10) Any other element determined relevant by the Commander.

(Added Pub. L. 117–263, div. A, title XV, §1502(a), Dec. 23, 2022, 136 Stat. 2879.)

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.

(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.—

(1) RAPID REPORTING.—The procedures established pursuant to subsection (a) shall require each cleared defense contractor to rapidly report to a component of the Department of Defense designated pursuant to subsection (a) of each successful penetration of the network or information systems of such contractor that meet the criteria established pursuant to subsection (b). Each such report shall include the following:

(A) A description of the technique or method used in such penetration.

(B) A sample of the malicious software, if discovered and isolated by the contractor, involved in such penetration.

(C) A summary of information created by or for the Department in connection with any Department program that has been potentially compromised due to such penetration.

(2) ACCESS TO EQUIPMENT AND INFORMATION BY DEPARTMENT OF DEFENSE PERSONNEL.—The procedures established pursuant to subsection (a) shall—

(A) include mechanisms for Department of Defense personnel to, upon request, obtain access to equipment or information of a cleared defense contractor necessary to conduct forensic analysis in addition to any analysis conducted by such contractor;

(B) provide that a cleared defense contractor is only required to provide access to equipment or information as described in subparagraph (A) to determine whether information created by or for the Department in connection with any Department program was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated; and

(C) provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person.

(3) DISSEMINATION OF INFORMATION.—The procedures established pursuant to subsection (a) shall limit the dissemination of information obtained or derived through such procedures to entities—

(A) with missions that may be affected by such information;

(B) that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(C) that conduct counterintelligence or law enforcement investigations; or

(D) for national security purposes, including cyber situational awareness and defense purposes.

(d) PROTECTION FROM LIABILITY OF CLEARED DEFENSE CONTRACTORS.—(1) No cause of action shall lie or be maintained in any court against any cleared defense contractor, and such action shall be promptly dismissed, for compliance with this section that is conducted in accordance with the procedures established pursuant to subsection (a).

(2)(A) Nothing in this section shall be construed—

(i) to require dismissal of a cause of action against a cleared defense contractor that has engaged in willful misconduct in the course of complying with the procedures established pursuant to subsection (a); or

(ii) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

(B) In any action claiming that paragraph (1) does not apply due to willful misconduct described in subparagraph (A), the plaintiff shall have the burden of proving by clear and convincing evidence the willful misconduct by each cleared defense contractor subject to such claim and that such willful misconduct proximately caused injury to the plaintiff.

(C) In this subsection, the term ''willful misconduct'' means an act or omission that is taken—

(i) intentionally to achieve a wrongful purpose;

(ii) knowingly without legal or factual justification; and

(iii) in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit.

(e) DEFINITIONS.—In this section:

(1) CLEARED DEFENSE CONTRACTOR.—The term ''cleared defense contractor'' means a private entity granted clearance by the Department of Defense to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the Department of Defense.

(2) COVERED NETWORK.—The term ''covered network'' means a network or information system of a cleared defense contractor that contains or processes information created by or for the Department of Defense with respect to which such contractor is required to apply enhanced protection.

(Added and amended Pub. L. 114–92, div. A, title XVI, §1641(a), Nov. 25, 2015, 129 Stat. 1114; Pub. L. 116–92, div. A, title IX, §902(8), title XVI, §1621(e)(1)(A)(vi), Dec. 20, 2019, 133 Stat. 1543, 1733; Pub. L. 116–283, div. A, title X, §1081(a)(15), Jan. 1, 2021, 134 Stat. 3871; Pub. L. 117–81, div. A, title X, §1081(a)(9), Dec. 27, 2021, 135 Stat. 1920.)

Editorial Notes

CODIFICATION

Section, as added and amended by Pub. L. 114–92, is based on Pub. L. 112–239, div. A, title IX, §941, Jan. 2, 2013, 126 Stat. 1889, which was formerly set out as a note under section 2224 of this title before being transferred to this chapter and renumbered as this section.

AMENDMENTS

2021—Subsec. (b)(2)(D). Pub. L. 117–81 inserted period at end.

Pub. L. 116–283 substituted ''of Defense for Intelligence and Security'' for ''of Defense for Intelligence.''

2019—Subsec. (b)(2)(B). Pub. L. 116–92, §902(8)(A), substituted ''Under Secretary of Defense for Acquisition and Sustainment'' for ''Under Secretary of Defense for Acquisition, Technology, and Logistics''.

Subsec. (b)(2)(C). Pub. L. 116–92, §1621(e)(1)(A)(vi), which directed amendment of subpar. (C) by substituting ''Under Secretary of Defense for Intelligence and Security'' for ''Under Secretary of Defense for Intelligence'', could not be executed because the words ''Under Secretary of Defense for Intelligence'' did not appear. Similar amendment was subsequently directed

to subpar. (D) by Pub. L. 116–283, see 2021 Amendment note above.

Pub. L. 116–92, § 902(8)(B), added subpar. (C). Former subpar. (C) redesignated (D).

Subsec. (b)(2)(D) to (F). Pub. L. 116–92, § 902(8)(C), redesignated subpars. (C) to (E) as (D) to (F), respectively.

2015—Pub. L. 114–92, § 1641(a)(1), substituted ''Reporting on penetrations of networks and information systems of certain contractors'' for ''Reports to Department of Defense on penetrations of networks and information systems of certain contractors'' in section catchline.

Pub. L. 114–92, § 1641(a), transferred section 941 of Pub. L. 112–239 to this chapter and renumbered it as this section. See Codification note above.

Subsec. (c)(3). Pub. L. 114–92, § 1641(a)(2), added par. (3) and struck out former par. (3). Prior to amendment, text read as follows: ''The procedures established pursuant to subsection (a) shall prohibit the dissemination outside the Department of Defense of information obtained or derived through such procedures that is not created by or for the Department except with the approval of the contractor providing such information.''

Subsec. (d). Pub. L. 114–92, § 1641(a)(3), added subsec. (d) and struck out former subsec. (d). Prior to amendment, text read as follows:

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act—

''(A) the Secretary of Defense shall establish the procedures required under subsection (a); and

''(B) the senior official designated under subsection (b)(1) shall establish the criteria required under such subsection.

''(2) APPLICABILITY DATE.—The requirements of this section shall apply on the date on which the Secretary of Defense establishes the procedures required under this section.''

§ 394. Authorities concerning military cyber operations

(a) IN GENERAL.—The Secretary of Defense shall develop, prepare, and coordinate; make ready all armed forces for purposes of; and, when appropriately authorized to do so, conduct, military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power.

(b) AFFIRMATION OF AUTHORITY.—Congress affirms that the activities or operations referred to in subsection (a), when appropriately authorized, include the conduct of military activities or operations in cyberspace short of hostilities (as such term is used in the War Powers Resolution (Public Law 93–148; 50 U.S.C. 1541 et seq.)) or in areas in which hostilities are not occurring, including for the purpose of preparation of the environment, information operations, force protection, and deterrence of hostilities, or counterterrorism operations involving the Armed Forces of the United States.

(c) CLANDESTINE ACTIVITIES OR OPERATIONS.—A clandestine military activity or operation in cyberspace shall be considered a traditional military activity for the purposes of section 503(e)(2) of the National Security Act of 1947 (50 U.S.C. 3093(e)(2)).

(d) CONGRESSIONAL OVERSIGHT.—The Secretary shall brief the congressional defense committees about any military activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, occurring during the previous quarter during the quarterly briefing required by section 484 of this title.

(e) RULE OF CONSTRUCTION.—Nothing in this section may be construed to limit the authority of the Secretary to conduct military activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to authorize specific military activities or operations, or to alter or otherwise affect the War Powers Resolution (50 U.S.C. 1541 et seq.), the Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note), or reporting of sensitive military cyber activities or operations required by section 395 of this title.

(f) DEFINITIONS.—In this section:

(1) The term ''clandestine military activity or operation in cyberspace'' means a military activity or military operation carried out in cyberspace, or associated preparatory actions, authorized by the President or the Secretary that—

(A) is marked by, held in, or conducted with secrecy, where the intent is that the activity or operation will not be apparent or acknowledged publicly; and

(B) is to be carried out—

(i) as part of a military operation plan approved by the President or the Secretary in anticipation of hostilities or as directed by the President or the Secretary;

(ii) to deter, safeguard, or defend against attacks or malicious cyber activities against the United States or Department of Defense information, networks, systems, installations, facilities, or other assets; or

(iii) in support of information related capabilities.

(2) The term ''foreign power'' has the meaning given such term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(3) The term ''United States person'' has the meaning given such term in such section.

(Added Pub. L. 114–92, div. A, title XVI, § 1642(a), Nov. 25, 2015, 129 Stat. 1116, § 130g; renumbered § 394 and amended Pub. L. 115–232, div. A, title XVI, §§ 1631(a), 1632, Aug. 13, 2018, 132 Stat. 2123.)

Editorial Notes

REFERENCES IN TEXT

The War Powers Resolution, referred to in subsecs. (b) and (e), is Pub. L. 93–148, Nov. 7, 1973, 87 Stat. 555, which is classified generally to chapter 33 (§ 1541 et seq.) of Title 50, War and National Defense. For complete classification of this Resolution to the Code, see Short Title note set out under section 1541 of Title 50 and Tables.

The Authorization for Use of Military Force, referred to in subsec. (e), is Pub. L. 107–40, Sept. 18, 2001, 115 Stat. 224, which is set out as a note under section 1541 of Title 50, War and National Defense.

AMENDMENTS

2018—Pub. L. 115–232, § 1632, designated existing provisions as subsec. (a), inserted heading, substituted ''conduct, military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response'' for ''conduct, a mili-

tary cyber operation in response'', struck out ''(as such terms are defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801))'' after ''foreign power'', and added subsecs. (b) to (f).

Pub. L. 115–232, §1631(a), renumbered section 130g of this title as this section.

Statutory Notes and Related Subsidiaries

SUPPORT FOR CYBER THREAT TABLETOP EXERCISE PROGRAM WITH THE DEFENSE INDUSTRIAL BASE

Pub. L. 118–159, div. A, title XV, §1504, Dec. 23, 2024, 138 Stat. 2133, provided that:

''(a) DEVELOPMENT OF CYBER THREAT TABLETOP EXERCISE PROGRAM.—

''(1) IN GENERAL.— Not later than one year after the date of the enactment of this Act [Dec. 23, 2024], the Secretary of Defense, acting through the Assistant Secretary of Defense for Cyber Policy, shall establish a program (to be known as the 'Cyber Threat Tabletop Exercise Program') to prepare the Department of Defense and the defense industrial base for cyber attacks preceding or during times of conflict or wars through the use of tabletop exercises.

''(2) PARTICIPATION.—

''(A) IN GENERAL.—In carrying out the program, the Secretary of Defense, acting through the Assistant Secretary of Defense for Cyber Policy, shall consult and coordinate with the following:

''(i) The Chief Information Officer of the Department of Defense.

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

''(iii) The Commander of the United States Cyber Command.

''(iv) The Commander of the United States Northern Command.

''(v) The Commander of the Army Interagency Training and Education Center.

''(vi) The Director of the Defense Cyber Crime Center.

''(vii) Such other individuals and entities as the Assistant Secretary of Defense for Cyber Policy determines appropriate.

''(B) SOLICITATION.—The Assistant Secretary of Defense for Cyber Policy may solicit such individuals and entities in the Department of Defense and the defense industrial base as the Assistant Secretary determines appropriate to participate in the program.

''(3) CYBER THREAT TABLETOP EXERCISE PROGRAM.——

''(A) IN GENERAL.—The program shall consist of the following:

''(i) A series of tabletop exercises that simulate cyber attack scenarios affecting the defense industrial base, which the Assistant Secretary of Defense for Cyber Policy shall carry out on a biannual basis beginning not later than one year after the date of the enactment of this Act until December 30, 2030, and in which the Department of Defense and entities in the defense industrial base shall participate.

''(ii) A series of tabletop exercises for use by individual entities or collections of entities in the defense industrial base that simulate cyber attack scenarios affecting the defense industrial base and which are designed to test and improve the responses and plans of such entities to such scenarios.

''(B) TABLETOP EXERCISE DEVELOPMENT.—

''(i) IN GENERAL.—The Assistant Secretary of Defense for Cyber Policy shall develop and update the tabletop exercises described in subparagraph (A).

''(ii) REALISTIC ATTACKS.—The Assistant Secretary of Defense for Cyber Policy shall ensure that the cyber attacks simulated by the tabletop exercises described in subparagraph (A) are based on the cyber attack capabilities and activities of current and potential adversaries of the United States.

''(4) PROCEDURES FOR IDENTIFICATION OF VULNERABILITIES AND LESSONS LEARNED.—Not later than one year after the date of the enactment of this Act, the Assistant Secretary of Defense for Cyber Policy shall establish procedures to—

''(A) identify vulnerabilities in the cybersecurity of the Department of Defense and the defense industrial base pursuant to the tabletop exercises carried out under the program; and

''(B) identify other lessons learned that can improve national security or the quality of such tabletop exercises.

''(b) ANNUAL REPORT.—Not later than September 30, 2025, and annually thereafter until the [sic] October 1, 2029, the Secretary of Defense, acting through the Assistant Secretary of Defense for Cyber Policy, shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report describing the activities of the Department of Defense pursuant to this section during the preceding year.

''(c) PROGRAM DEFINED.—In this section, the term 'program' means the program established under subsection (a).''

AUTHORITY FOR COUNTERING ILLEGAL TRAFFICKING BY MEXICAN TRANSNATIONAL CRIMINAL ORGANIZATIONS IN CYBERSPACE

Pub. L. 118–31, div. A, title XV, §1505, Dec. 22, 2023, 137 Stat. 539, provided that:

''(a) AUTHORITY.—In accordance with sections 124 and 394 of title 10, United States Code, the Secretary of Defense, in support of and in coordination with the heads of other relevant Federal departments and agencies and in consultation with the Government of Mexico as appropriate, may conduct detection, monitoring, and other operations in cyberspace to counter Mexican transnational criminal organizations that are engaged in any of the following activities that cross the southern border of the United States:

''(1) Smuggling of illegal drugs, controlled substances, or precursors thereof.

''(2) Human trafficking.

''(3) Weapons trafficking.

''(4) Other illegal activities.

''(b) CERTAIN ENTITIES.—The authority under paragraph (1) [probably should be ''subsection (a)''] may be used to counter Mexican transnational criminal organizations, including entities cited in the most recent National Drug Threat Assessment published by the United States Drug Enforcement Administration, that are engaged in any of the activities described in such paragraph.''

MANAGEMENT OF DATA ASSETS BY CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER

Pub. L. 118–31, div. A, title XV, §1523, Dec. 22, 2023, 137 Stat. 553, provided that:

''(a) IN GENERAL.—The Secretary of Defense, subject to existing authorities and limitations and acting through the Chief Digital and Artificial Intelligence Officer of the Department of Defense, shall provide the digital infrastructure and procurement vehicles necessary to manage data assets and data analytics capabilities at scale to enable an understanding of foreign key terrain and relational frameworks in cyberspace to support the planning of cyber operations, the generation of indications and warnings regarding military operations and capabilities, and the calibration of actions and reactions in strategic competition.

''(b) RESPONSIBILITIES OF CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER.—The Chief Digital and Artificial Intelligence Officer shall—

''(1) develop a baseline of data assets exclusive to foreign key terrain and relational frameworks in cyberspace maintained by the intelligence agencies of

the Department of Defense, the military departments, the combatant commands, and any other components of the Department of Defense;

''(2) develop and oversee the implementation of plans to enhance such data assets that the Chief Digital and Artificial Intelligence Officer determines are essential to support the purposes set forth in subsection (a); and

''(3) ensure that such activities and plans are undertaken in cooperation and in coordination with the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, to ensure that any data collection, procurement, acquisition, use, or retention measure conducted pursuant to this section is in compliance with applicable laws and regulations, including standards pertaining to data related to United States persons or any persons in the United States.

''(c) OTHER MATTERS.—The Chief Digital and Artificial Intelligence Officer shall—

''(1) designate or establish one or more Department of Defense executive agents for enhancing data assets and the acquisition of data analytic tools for users;

''(2) ensure that data assets referred to in subsection (b) that are in the possession of a component of the Department of Defense are accessible for the purposes described in subsection (a); and

''(3) ensure that advanced analytics, including artificial intelligence technology, are developed and applied to the analysis of the data assets referred to in subsection (b) in support of the purposes described in subsection (a).

''(d) SEMIANNUAL BRIEFINGS.—Not later than 120 days after the date of the enactment of this Act [Dec. 22, 2023], and not less frequently than semiannually thereafter, the Chief Digital and Artificial Intelligence Officer shall provide to the appropriate congressional committees a briefing on the implementation of this section.

''(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to authorize the Department of Defense to collect, procure, or otherwise acquire data, including commercially available data, in any manner that is not authorized by law, or to make use of data assets in any manner, or for any purpose, that is not otherwise authorized by law.

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

''(1) the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives];

''(2) the Permanent Select Committee on Intelligence of the House of Representatives; and

''(3) the Select Committee on Intelligence of the Senate.''

PROTECTION OF CRITICAL INFRASTRUCTURE

Pub. L. 117–263, div. A, title XV, § 1511, Dec. 23, 2022, 136 Stat. 2892, provided that:

''(a) IN GENERAL.—In the event that the President determines that there is an active, systematic, and ongoing campaign of attacks in cyberspace by a foreign power against the Government or the critical infrastructure of the United States, the President may authorize the Secretary of Defense, acting through the Commander of the United States Cyber Command, to conduct military cyber activities or operations pursuant to section 394 of title 10, United States Code, in foreign cyberspace to deter, safeguard, or defend against such attacks.

''(b) AFFIRMATION OF SCOPE OF CYBER ACTIVITIES OR OPERATIONS.—Congress affirms that the cyber activities or operations referred to in subsection (a), when appropriately authorized, shall be conducted consistent with section 394 of title 10, United States Code.

''(c) DEFINITION OF CRITICAL INFRASTRUCTURE.—In this section, the term 'critical infrastructure' has the meaning given that term in subsection (e) [of section 1016] of the Critical Infrastructure[s] Protection Act of 2001 (42 U.S.C. 5195c(e)).''

OPERATIONAL TECHNOLOGY AND MISSION-RELEVANT TERRAIN IN CYBERSPACE

Pub. L. 117–81, div. A, title XV, § 1505, Dec. 27, 2021, 135 Stat. 2023, as amended by Pub. L. 118–31, div. A, title XV, § 1502(a)(2)(E), Dec. 22, 2023, 137 Stat. 538, provided that:

''(a) MISSION-RELEVANT TERRAIN.—Not later than January 1, 2025, the Secretary of Defense shall complete mapping of mission-relevant terrain in cyberspace for Defense Critical Assets and Task Critical Assets at sufficient granularity to enable mission thread analysis and situational awareness, including required—

''(1) decomposition of missions reliant on such Assets;

''(2) identification of access vectors;

''(3) internal and external dependencies;

''(4) topology of networks and network segments;

''(5) cybersecurity defenses across information and operational technology on such Assets; and

''(6) identification of associated or reliant weapon systems.

''(b) COMBATANT COMMAND RESPONSIBILITIES.—Not later than January 1, 2024, the Commanders of 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, and other relevant Commands, in coordination with the Commander of United States Cyber Command, in order to enable effective mission thread analysis, cyber situational awareness, and effective cyber defense of Defense Critical Assets and Task Critical Assets under their control or in their areas of responsibility, shall develop, institute, and make necessary modifications to—

''(1) internal combatant command processes, responsibilities, and functions;

''(2) coordination with service components under their operational control, United States Cyber Command, Joint Forces Headquarters-Department of Defense Information Network, and the service cyber components;

''(3) combatant command headquarters' situational awareness posture to ensure an appropriate level of cyber situational awareness of the forces, facilities, installations, bases, critical infrastructure, and weapon systems under their control or in their areas of responsibility, including, in particular, Defense Critical Assets and Task Critical Assets; and

''(4) documentation of their mission-relevant terrain in cyberspace.

''(c) DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER RESPONSIBILITIES.—

''(1) IN GENERAL.—Not later than November 1, 2023, the Chief Information Officer of the Department of Defense shall establish or make necessary changes to policy, control systems standards, risk management framework and authority to operate policies, and cybersecurity reference architectures to provide baseline cybersecurity requirements for operational technology in forces, facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network.

''(2) IMPLEMENTATION OF POLICIES.—The Chief Information Officer of the Department of Defense shall leverage acquisition guidance, concerted assessment of the Department's operational technology enterprise, and coordination with the military department principal cyber advisors and chief information officers to drive necessary change and implementation of relevant policy across the Department's forces, facilities, installations, bases, critical infrastructure, and weapon systems.

''(3) ADDITIONAL RESPONSIBILITIES.—The Chief Information Officer of the Department of Defense shall ensure that policies, control systems standards, and cybersecurity reference architectures—

''(A) are implementable by components of the Department;

''(B) limit adversaries' ability to reach or manipulate control systems through cyberspace;

''(C) appropriately balance non-connectivity and monitoring requirements;

''(D) include data collection and flow requirements;

''(E) interoperate with and are informed by the operational community's workflows for defense of information and operational technology in the forces, facilities, installations, bases, critical infrastructure, and weapon systems across the Department;

''(F) integrate and interoperate with Department mission assurance construct; and

''(G) are implemented with respect to Defense Critical Assets and Task Critical Assets.

''(d) UNITED STATES CYBER COMMAND OPERATIONAL RESPONSIBILITIES.—Not later than January 1, 2025, the Commander of United States Cyber Command shall make necessary modifications to the mission, scope, and posture of Joint Forces Headquarters-Department of Defense Information Network to ensure that Joint Forces Headquarters—

''(1) has appropriate visibility of operational technology in the forces, facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network, including, in particular, Defense Critical Assets and Task Critical Assets;

''(2) can effectively command and control forces to defend such operational technology; and

''(3) has established processes for—

''(A) incident and compliance reporting;

''(B) ensuring compliance with Department of Defense cybersecurity policy; and

''(C) ensuring that cyber vulnerabilities, attack vectors, and security violations, including, in particular, those specific to Defense Critical Assets and Task Critical Assets, are appropriately managed.

''(e) UNITED STATES CYBER COMMAND FUNCTIONAL RESPONSIBILITIES.—Not later than January 1, 2025, the Commander of United States Cyber Command shall—

''(1) ensure in its role of Joint Forces Trainer for the Cyberspace Operations Forces that operational technology cyber defense is appropriately incorporated into training for the Cyberspace Operations Forces;

''(2) delineate the specific force composition requirements within the Cyberspace Operations Forces for specialized cyber defense of operational technology, including the number, size, scale, and responsibilities of defined Cyber Operations Forces elements;

''(3) develop and maintain, or support the development and maintenance of, a joint training curriculum for operational technology-focused Cyberspace Operations Forces;

''(4) support the Chief Information Officer of the Department of Defense as the Department's senior official for the cybersecurity of operational technology under this section;

''(5) develop and institutionalize, or support the development and institutionalization of, tradecraft for defense of operational technology across local defenders, cybersecurity service providers, cyber protection teams, and service-controlled forces;

''(6) develop and institutionalize integrated concepts of operation, operational workflows, and cybersecurity architectures for defense of information and operational technology in the forces, facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network, including, in particular, Defense Critical Assets and Task Critical Assets, including—

''(A) deliberate and strategic sensoring of such Network and Assets;

''(B) instituting policies governing connections across and between such Network and Assets;

''(C) modelling of normal behavior across and between such Network and Assets;

''(D) engineering data flows across and between such Network and Assets;

''(E) developing local defenders, cybersecurity service providers, cyber protection teams, and service-controlled forces' operational workflows and tactics, techniques, and procedures optimized for the designs, data flows, and policies of such Network and Assets;

''(F) instituting of model defensive cyber operations and Department of Defense Information Network operations tradecraft; and

''(G) integrating of such operations to ensure interoperability across echelons; and

''(7) advance the integration of the Department of Defense's mission assurance, cybersecurity compliance, cybersecurity operations, risk management framework, and authority to operate programs and policies.

''(f) SERVICE RESPONSIBILITIES.—Not later than January 1, 2025, the Secretaries of the military departments, through the service principal cyber advisors, chief information officers, the service cyber components, and relevant service commands, shall make necessary investments in operational technology in the forces, facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network and the service-controlled forces responsible for defense of such operational technology to—

''(1) ensure that relevant local network and cybersecurity forces are responsible for defending operational technology across the forces, facilities, installations, bases, critical infrastructure, and weapon systems, including, in particular, Defense Critical Assets and Task Critical Assets;

''(2) ensure that relevant local operational technology-focused system operators, network and cybersecurity forces, mission defense teams and other service-retained forces, and cyber protection teams are appropriately trained, including through common training and use of cyber ranges, as appropriate, to execute the specific requirements of cybersecurity operations in operational technology;

''(3) ensure that all Defense Critical Assets and Task Critical Assets are monitored and defended by Cybersecurity Service Providers;

''(4) ensure that operational technology is appropriately sensored and appropriate cybersecurity defenses, including technologies associated with the More Situational Awareness for Industrial Control Systems Joint Capability Technology Demonstration, are employed to enable defense of Defense Critical Assets and Task Critical Assets;

''(5) implement Department of Defense Chief Information Officer policy germane to operational technology, including, in particular, with respect to Defense Critical Assets and Task Critical Assets;

''(6) plan for, designate, and train dedicated forces to be utilized in operational technology-centric roles across the military services and United States Cyber Command; and

''(7) ensure that operational technology, as appropriate, is not easily accessible via the internet and that cybersecurity investments accord with mission risk to and relevant access vectors for Defense Critical Assets and Task Critical Assets.

''(g) OFFICE OF THE SECRETARY OF DEFENSE RESPONSIBILITIES.—Not later than January 1, 2023, the Secretary of Defense shall—

''(1) assess and finalize Office of the Secretary of Defense components' roles and responsibilities for the cybersecurity of operational technology in the forces, facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network;

''(2) assess the need to establish centralized or dedicated funding for remediation of cybersecurity gaps in operational technology across the Department of Defense Information Network;

''(3) make relevant modifications to the Department of Defense's mission assurance construct, Mis-

sion Assurance Coordination Board, and other relevant bodies to drive—

''(A) prioritization of kinetic and non-kinetic threats to the Department's missions and minimization of mission risk in the Department's war plans;

''(B) prioritization of relevant mitigations and investments to harden and assure the Department's missions and minimize mission risk in the Department's war plans; and

''(C) completion of mission relevant terrain mapping of Defense Critical Assets and Task Critical Assets and population of associated assessment and mitigation data in authorized repositories;

''(4) make relevant modifications to the Strategic Cybersecurity Program; and

''(5) drive and provide oversight of the implementation of this section.

''(h) IMPLEMENTATION.—

''(1) IN GENERAL.—In implementing this section, the Secretary of Defense shall prioritize the cybersecurity and cyber defense of Defense Critical Assets and Task Critical Assets and shape cyber investments, policy, operations, and deployments to ensure cybersecurity and cyber defense.

''(2) APPLICATION.—This section shall apply to assets owned and operated by the Department of Defense, as well as to applicable non-Department assets essential to the projection, support, and sustainment of military forces and operations worldwide.

''(i) DEFINITION.—In this section:

''(1) MISSION-RELEVANT TERRAIN IN CYBERSPACE.—'mission-relevant [sic] terrain in cyberspace' has the meaning given such term as specified in Joint Publication 6-0.

''(2) OPERATIONAL TECHNOLOGY.—The term 'operational technology' means control systems or controllers, communication architectures, and user interfaces that monitor or control infrastructure and equipment operating in various environments, such as weapon systems, utility or energy production and distribution, or medical, logistics, nuclear, biological, chemical, or manufacturing facilities.''

FRAMEWORK FOR CYBER HUNT FORWARD OPERATIONS

Pub. L. 116–283, div. A, title XVII, §1720, Jan. 1, 2021, 134 Stat. 4107, provided that:

''(a) FRAMEWORK REQUIRED.—Not later than April 1, 2021, the Secretary of Defense shall develop a standard, comprehensive framework to enhance the consistency, execution, and effectiveness of cyber hunt forward operations.

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

''(1) Identification of the selection criteria for proposed cyber hunt forward operations, including specification of necessary thresholds for the justification of operations and thresholds for partner cooperation.

''(2) The roles and responsibilities of the following organizations in the support of the planning and execution of cyber hunt forward operations:

''(A) United States Cyber Command.

''(B) Service cyber components.

''(C) The Office of the Under Secretary of Defense for Policy.

''(D) Geographic combatant commands.

''(E) Cyber Operations-Integrated Planning Elements and Joint Cyber Centers.

''(F) Embassies and consulates of the United States.

''(3) Pre-deployment planning guidelines to maximize the operational success of each unique operation, including guidance that takes into account the highly variable nature of the following aspects at the tactical level:

''(A) Team composition, including necessary skillsets [sic], recommended training, and guidelines on team size and structure.

''(B) Relevant factors to determine mission duration in a country of interest.

''(C) Agreements with partner countries required pre-deployment.

''(D) Criteria for potential follow-on operations.

''(E) Equipment and infrastructure required to support the missions.

''(4) Metrics to measure the effectiveness of each operation, including means to evaluate the value of discovered malware and infrastructure, the effect on the adversary, and the potential for future engagements with the partner country.

''(5) Roles and responsibilities for United States Cyber Command and the National Security Agency in the analysis of relevant mission data.

''(6) A detailed description of counterintelligence support for cyber hunt forward operations.

''(7) A standardized force presentation model across service components and combatant commands.

''(8) Review of active and reserve component personnel policies to account for deployment and redeployment operations, including the following:

''(A) Global Force Management.

''(B) Contingency, Exercise, and Deployment orders to be considered for and applied towards deployment credit and benefits.

''(9) Such other matters as the Secretary determines relevant.

''(c) BRIEFING.—

''(1) IN GENERAL.—Not later than May 1, 2021, the Secretary of Defense shall provide to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives a briefing on the framework developed pursuant to subsection (a).

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

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

''(B) An explanation of the tradeoffs associated with the use of Department of Defense resources for cyber hunt forward missions in the context of competing priorities.

''(C) Such recommendations as the Secretary may have for legislative action to improve the effectiveness of cyber hunt forward missions.''

TAILORED CYBERSPACE OPERATIONS ORGANIZATIONS

Pub. L. 116–283, div. A, title XVII, §1723, Jan. 1, 2021, 134 Stat. 4110, as amended by Pub. L. 117–263, div. A, title XV, §1504, Dec. 23, 2022, 136 Stat. 2880, provided that:

''(a) STUDY.—

''(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act [Jan. 1, 2021], the Secretary of the Navy and the Chief of Naval Operations, in consultation with the Commander of 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] a study of the Navy Cyber Warfare Development Group (NCWDG).

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

''(A) An examination of NCWDG's structure, manning, authorities, funding, and operations.

''(B) A review of organizational relationships—

''(i) within the Navy; and

''(ii) to other Department of Defense organizations, as well as non-Department of Defense organizations.

''(C) Recommendations for how the NCWDG can be strengthened and improved, without growth in size.

''(D) Such other information as determined necessary or appropriate by the Secretary of the Navy.

''(3) RELEASE.—

''(A) TO CONGRESS.—Not later than 7 days after completion of the study required under paragraph (1), the Secretary of the Navy shall brief the congressional defense committees on the findings of the study.

''(B) TO SERVICE SERVICES.— The Secretary of the Navy shall transmit to the secretaries of the military services and the Assistant Secretary of Defense for Special Operations and Irregular Warfare the study required under paragraph (1).

''(b) DESIGNATION.—Notwithstanding any other provision of law, the Secretary of the Navy shall designate the NCWDG as a screened command.

''(c) AUTHORITY TO REPLICATE.—After review of the study required under subsection (a) and consulting the Commander of United States Cyber Command in accordance with procedures established by the Secretary of Defense, the secretaries of the military services may establish tailored cyberspace operations organizations of comparable size to NCWDG within the military service, respectively, of each such secretary. Such counterpart organizations shall have the same authorities as the NCWDG. On behalf of United States Special Operations Command, the Assistant Secretary of Defense for Special Operations and Irregular Warfare may authorize a tailored cyberspace operations organization within United States Special Operations Command of similar size and equivalent authorities as NCWDG.

''(d) BRIEFING TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act, the secretaries of the military services and the Assistant Secretary of Defense for Special Operations and Irregular Warfare shall brief the congressional defense committees on—

''(1) the utilization of the authority provided pursuant to subsection (c); and

''(2) if appropriate based on such utilization, details on how the military service, respectively, of each such secretary intends to establish tailored cyberspace operations organizations.

''(e) IMPLEMENTATION.—Not later than May 1, 2023, the Commanding Officer of Navy Cyber Warfare Development Group shall submit to the congressional defense committees an independent review of the study under subsection (a). The review shall include, at a minimum, evaluations of—

''(1) the value of the study to the Navy Cyber Warfare Development Group and to the Navy;

''(2) any recommendations not considered or included as part of the study;

''(3) the implementation of subsection (b); and

''(4) other matters as determined by the Commanding Officer.

''(f) UPDATE TO CONGRESS.—Not later than July 1, 2023, the Secretaries of the military departments and the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict shall provide to the congressional defense committees a briefing on activities taken during the period following the date of the briefing provided under subsection (d), including an examination of establishing Tailored Cyberspace Operations Organizations and use of the authority provided pursuant to subsection (c).

''(g) AIR FORCE ACTIONS.—Not later than July 1, 2023, the Secretary of the Air Force shall submit to the congressional defense committees a review of the activities of the Navy Cyber Warfare Development Group, including with respect to the authorities of the Group. The review shall include the following:

''(1) An assessment of whether such authorities shall be conferred on the 90th Cyberspace Operations Squadron of the Air Force.

''(2) A consideration of whether the 90th Cyberspace Operations Squadron should be designated a controlled tour, as defined by the Secretary.''

NOTIFICATION OF DELEGATION OF AUTHORITIES TO THE SECRETARY OF DEFENSE FOR MILITARY OPERATIONS IN CYBERSPACE

Pub. L. 116–92, div. A, title XVI, §1642, Dec. 20, 2019, 133 Stat. 1751, provided that:

''(a) IN GENERAL.—The Secretary of Defense shall provide written notification to the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate of the following:

''(1) Authorities delegated to the Secretary by the President for military operations in cyberspace that are otherwise held by the National Command Authority, not later than 15 days after any such delegation. A notification under this paragraph shall include a description of the authorities delegated to the Secretary.

''(2) Concepts of operations approved by the Secretary pursuant to delegated authorities described in paragraph (1), not later than 15 days after any such approval. A notification under this paragraph shall include the following:

''(A) A description of authorized activities to be conducted or planned to be conducted pursuant to such authorities.

''(B) The defined military objectives relating to such authorities.

''(C) A list of countries in which such authorities may be exercised.

''(D) A description of relevant orders issued by the Secretary in accordance with such authorities.

''(b) PROCEDURES.—

''(1) IN GENERAL.—The Secretary of Defense shall establish and submit to the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate procedures for complying with the requirements of subsection (a), consistent with the national security of the United States and the protection of operational integrity. The Secretary shall promptly notify such committees in writing of any changes to such procedures at least 14 days prior to the adoption of any such changes.

''(2) SUFFICIENCY.—The Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate shall ensure that committee procedures designed to protect from unauthorized disclosure classified information relating to national security of the United States are sufficient to protect the information that is submitted to such committees pursuant to this section.

''(3) NOTIFICATION IN EVENT OF UNAUTHORIZED DISCLOSURE.—In the event of an unauthorized disclosure of authorities covered by this section, the Secretary of Defense shall ensure, to the maximum extent practicable, that the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate are notified immediately. Notification under this paragraph may be verbal or written, but in the event of a verbal notification, a written notification signed by the Secretary shall be provided by not later than 48 hours after the provision of such verbal notification.''

ANNUAL MILITARY CYBERSPACE OPERATIONS REPORT

Pub. L. 116–92, div. A, title XVI, §1644, Dec. 20, 2019, 133 Stat. 1752, as amended by Pub. L. 118–31, div. A, title X, §1061(d), Dec. 22, 2023, 137 Stat. 399, provided that:

''(a) IN GENERAL.—Not later than March 1 of each year, the Secretary of Defense shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a written report summarizing all named military cyberspace effects operations conducted in the previous calendar year, including cyber effects conducted for either offensive or defensive purposes. Each such summary should be organized by adversarial country and should include the following for each named operation:

''(1) An identification of the objective and purpose.

''(2) Descriptions of the impacted countries, organizations, or forces, and nature of the impact.

''(3) A description of methodologies used for the cyber effects operation or cyber effects enabling operation.

''(4) An identification of the Cyber Mission Force teams, or other Department of Defense entity or units, that conducted such operation, and supporting teams, entities, or units.

''(5) An identification of the infrastructures on which such operations occurred.

''(6) A description of relevant legal, operational, and funding authorities.

''(7) Additional costs beyond baseline operations and maintenance and personnel costs directly associated with the conduct of the cyber effects operation or cyber effects enabling operation.

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

''(b) CLASSIFICATION.—The Secretary of Defense shall provide each report required under subsection (a) at a classification level the Secretary determines appropriate.

''(c) LIMITATION.—This section does not apply to cyber-enabled military information support operations or military deception operations or cyber effects operations for which Congress has otherwise been provided notice.''

POLICY OF THE UNITED STATES ON CYBERSPACE, CYBERSECURITY, CYBER WARFARE, AND CYBER DETERRENCE

Pub. L. 115–232, div. A, title XVI, §1636, Aug. 13, 2018, 132 Stat. 2126, provided that:

''(a) IN GENERAL.—It shall be the policy of the United States, with respect to matters pertaining to cyberspace, cybersecurity, and cyber warfare, that the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities of foreign powers that target United States interests with the intent to—

''(1) cause casualties among United States persons or persons of United States allies;

''(2) significantly disrupt the normal functioning of United States democratic society or government (including attacks against critical infrastructure that could damage systems used to provide key services to the public or government);

''(3) threaten the command and control of the Armed Forces, the freedom of maneuver of the Armed Forces, or the industrial base or other infrastructure on which the United States Armed Forces rely to defend United States interests and commitments; or

''(4) achieve an effect, whether individually or in aggregate, comparable to an armed attack or imperil a vital interest of the United States.

''(b) RESPONSE OPTIONS.—In carrying out the policy set forth in subsection (a), the United States shall plan, develop, and, when appropriate, demonstrate response options to address the full range of potential cyber attacks on United States interests that could be conducted by potential adversaries of the United States.

''(c) DENIAL OPTIONS.—In carrying out the policy set forth in subsection (a) through response options developed pursuant to subsection (b), the United States shall, to the greatest extent practicable, prioritize the defensibility and resiliency against cyber attacks and malicious cyber activities described in subsection (a) of infrastructure critical to the political integrity, economic security, and national security of the United States.

''(d) COST-IMPOSITION OPTIONS.—In carrying out the policy set forth in subsection (a) through response options developed pursuant to subsection (b), the United States shall develop and, when appropriate, demonstrate, or otherwise make known to adversaries the existence of, cyber capabilities to impose costs on any foreign power targeting the United States or United States persons with a cyber attack or malicious cyber activity described in subsection (a).

''(e) MULTI-PRONG RESPONSE.—In carrying out the policy set forth in subsection (a) through response options developed pursuant to subsection (b), the United States shall leverage all instruments of national power.

''(f) UPDATE ON PRESIDENTIAL POLICY.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Aug. 13, 2018], the President shall transmit, in unclassified and classified forms, as appropriate, to the appropriate congressional committees a report containing an update to the report provided to the Congress on the policy of the United States on cyberspace, cybersecurity, and cyber warfare pursuant to section 1633 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 10 U.S.C. 130g note) [now 10 U.S.C. 394 note].

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

''(A) An assessment of the current posture in cyberspace, including assessments of—

''(i) whether past responses to major cyber attacks have had the desired deterrent effect; and

''(ii) how adversaries have responded to past United States responses.

''(B) Updates on the Administration's efforts in the development of—

''(i) cost imposition strategies;

''(ii) varying levels of cyber incursion and steps taken to date to prepare for the imposition of the consequences referred to in clause (i); and

''(iii) the Cyber Deterrence Initiative.

''(C) Information relating to the Administration's plans, including specific planned actions, regulations, and legislative action required, for—

''(i) advancing technologies in attribution, inherently secure technology, and artificial intelligence society-wide;

''(ii) improving cybersecurity in and cooperation with the private sector;

''(iii) improving international cybersecurity cooperation; and

''(iv) implementing the policy referred to in paragraph (1), including any realignment of government or government responsibilities required, writ large.

''(f) [probably should be ''(g)''] RULE OF CONSTRUCTION.—Nothing in this subsection may be construed to limit the authority of the President or Congress to authorize the use of military force.

''(g) [probably should be ''(h)''] DEFINITIONS.—In this section:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives];

''(B) the Permanent Select Committee on Intelligence of the House of Representatives;

''(C) the Select Committee on Intelligence of the Senate;

''(D) the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on the Judiciary of the House of Representatives; and

''(E) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, and the Committee on the Judiciary of the Senate.

''(2) FOREIGN POWER.—The term 'foreign power' has the meaning given such term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).''

Pub. L. 115–91, div. A, title XVI, §1633, Dec. 12, 2017, 131 Stat. 1738, provided that:

''(a) IN GENERAL.—The President shall—

''(1) develop a national policy for the United States relating to cyberspace, cybersecurity, and cyber warfare; and

''(2) submit to the appropriate congressional committees a report on the policy.

''(b) ELEMENTS.—The national policy required under subsection (a) shall include the following elements:

''(1) Delineation of the instruments of national power available to deter or respond to cyber attacks or other malicious cyber activities by a foreign power or actor that targets United States interests.

''(2) Available or planned response options to address the full range of potential cyber attacks on United States interests that could be conducted by potential adversaries of the United States.

''(3) Available or planned denial options that prioritize the defensibility and resiliency against cyber attacks and malicious cyber activities that are carried out against infrastructure critical to the political integrity, economic security, and national security of the United States.

''(4) Available or planned cyber capabilities that may be used to impose costs on any foreign power targeting the United States or United States persons with a cyber attack or malicious cyber activity.

''(5) Development of multi-prong response options, such as—

''(A) boosting the cyber resilience of critical United States strike systems (including cyber, nuclear, and non-nuclear systems) in order to ensure the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attack;

''(B) developing offensive cyber capabilities and specific plans and strategies to put at risk targets most valued by adversaries of the United States and their key decision makers; and

''(C) enhancing attribution capabilities and developing intelligence and offensive cyber capabilities to detect, disrupt, and potentially expose malicious cyber activities.

''(c) LIMITATION ON AVAILABILITY OF FUNDS.—

''(1) IN GENERAL.—Of the funds authorized to be appropriated by this Act [see Tables for classification] or otherwise made available for fiscal year 2018 for procurement, research, development, test and evaluation, and operations and maintenance, for the covered activities of the Defense Information Systems Agency, not more than 60 percent may be obligated or expended until the date on which the President submits to the appropriate congressional committees the report under subsection (a)(2).

''(2) COVERED ACTIVITIES DESCRIBED.—The covered activities referred to in paragraph (1) are the activities of the Defense Information Systems Agency in support of—

''(A) the White House Communication Agency; and

''(B) the White House Situation Support Staff.

''(d) DEFINITIONS.—In this section:

''(1) The term 'foreign power' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

''(2) The term 'appropriate congressional committees' means—

''(A) the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives];

''(B) the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on the Judiciary of the House of Representatives; and

''(C) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, and the Committee on the Judiciary of the Senate.''

ACTIVE DEFENSE AGAINST THE RUSSIAN FEDERATION, PEOPLE'S REPUBLIC OF CHINA, DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA, AND ISLAMIC REPUBLIC OF IRAN ATTACKS IN CYBERSPACE

Pub. L. 115–232, div. A, title XVI, §1642, Aug. 13, 2018, 132 Stat. 2132, provided that:

''(a) AUTHORITY TO DISRUPT, DEFEAT, AND DETER CYBER ATTACKS.—

''(1) IN GENERAL.—In the event that the National Command Authority determines that the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, or Islamic Republic of Iran is conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes, the National Command Authority may authorize the Secretary of Defense, acting through the Commander of the United States Cyber Command, to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter such attacks under the authority and policy of the Secretary of Defense to conduct cyber operations and information operations as traditional military activities.

''(2) NOTIFICATION AND REPORTING.—

''(A) NOTIFICATION OF OPERATIONS.—In exercising the authority provided in paragraph (1), the Secretary shall provide notices to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] in accordance with section 395 of title 10, United States Code (as transferred and redesignated pursuant to section 1631).

''(B) QUARTERLY REPORTS BY COMMANDER OF THE UNITED STATES CYBER COMMAND.—

''(i) IN GENERAL.—In any fiscal year in which the Commander of the United States Cyber Command carries out an action under paragraph (1), the Secretary of Defense shall, not less frequently than quarterly, submit to the congressional defense committees a report on the actions of the Commander under such paragraph in such fiscal year.

''(ii) MANNER OF REPORTING.—Reports submitted under clause (i) shall be submitted in a manner that is consistent with the recurring quarterly report required by section 484 of title 10, United States Code.

''(b) PRIVATE SECTOR COOPERATION.—The Secretary may make arrangements with private sector entities, on a voluntary basis, to share threat information related to malicious cyber actors, and any associated false online personas or compromised infrastructure, associated with a determination under subsection (a)(1), consistent with the protection of sources and methods and classification guidelines, as necessary.

''(c) ANNUAL REPORT.—Not less frequently than once each year, the Secretary shall submit to the congressional defense committees, the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), the Committee on Foreign Affairs of the House of Representatives, and the Committee on Foreign Relations of the Senate a report on—

''(1) the scope and intensity of the information operations and attacks through cyberspace by the countries specified in subsection (a)(1) against the government or people of the United States observed by the cyber mission forces of the United States Cyber Command and the National Security Agency; and

''(2) adjustments of the Department of Defense in the response directed or recommended by the Secretary with respect to such operations and attacks.

''(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

''(1) limit the authority of the Secretary to conduct military activities or operations in cyberspace, including clandestine activities or operations in cyberspace; or

''(2) affect the War Powers Resolution (Public Law 93–148; 50 U.S.C. 1541 et seq.) or the Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note).''

PILOT PROGRAM TO MODEL CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

Pub. L. 115–232, div. A, title XVI, §1649, Aug. 13, 2018, 132 Stat. 2137, provided that:

''(a) PILOT PROGRAM REQUIRED.—

''(1) IN GENERAL.—The Assistant Secretary of Defense for Homeland Defense and Global Security shall carry out a pilot program to model cyber attacks on critical infrastructure in order to identify and develop means of improving Department of Defense responses to requests for defense support to civil authorities for such attacks.

''(2) RESEARCH EXERCISES.—The pilot program shall source data from and include consideration of the

'Jack Voltaic' research exercises conducted by the Army Cyber Institute, industry partners of the Institute, and the cities of New York, New York, and Houston, Texas.

''(b) PURPOSE.—The purpose of the pilot program shall be to accomplish the following:

''(1) The development and demonstration of risk analysis methodologies, and the application of commercial simulation and modeling capabilities, based on artificial intelligence and hyperscale cloud computing technologies, as applicable—

''(A) to assess defense critical infrastructure vulnerabilities and interdependencies to improve military resiliency;

''(B) to determine the likely effectiveness of attacks described in subsection (a)(1), and countermeasures, tactics, and tools supporting responsive military homeland defense operations;

''(C) to train personnel in incident response;

''(D) to conduct exercises and test scenarios;

''(E) to foster collaboration and learning between and among departments and agencies of the Federal Government, State and local governments, and private entities responsible for critical infrastructure; and

''(F) improve intra-agency and inter-agency coordination for consideration and approval of requests for defense support to civil authorities.

''(2) The development and demonstration of the foundations for establishing and maintaining a program of record for a shared high-fidelity, interactive, affordable, cloud-based modeling and simulation of critical infrastructure systems and incident response capabilities that can simulate complex cyber and physical attacks and disruptions on individual and multiple sectors on national, regional, State, and local scales.

''(c) REPORT.—

''(1) IN GENERAL.—At the same time the budget of the President for fiscal year 2021 is submitted to Congress pursuant to section 1105(a) of title 31, United States Code, the Assistant Secretary shall, in consultation with the Secretary of Homeland Security, submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the pilot program.

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

''(A) A description of the results of the pilot program as of the date of the report.

''(B) A description of the risk analysis methodologies and modeling and simulation capabilities developed and demonstrated pursuant to the pilot program, and an assessment of the potential for future growth of commercial technology in support of the homeland defense mission of the Department of Defense.

''(C) Such recommendations as the Secretary considers appropriate regarding the establishment of a program of record for the Department on further development and sustainment of risk analysis methodologies and advanced, large-scale modeling and simulation on critical infrastructure and cyber warfare.

''(D) Lessons learned from the use of novel risk analysis methodologies and large-scale modeling and simulation carried out under the pilot program regarding vulnerabilities, required capabilities, and reconfigured force structure, coordination practices, and policy.

''(E) Planned steps for implementing the lessons described in subparagraph (D).

''(F) Any other matters the Secretary determines appropriate.''

IDENTIFICATION OF COUNTRIES OF CONCERN REGARDING CYBERSECURITY

Pub. L. 115–232, div. A, title XVI, §1654, Aug. 13, 2018, 132 Stat. 2148, provided that:

''(a) IDENTIFICATION OF COUNTRIES OF CONCERN.—Not later than 180 days after the date of the enactment of this Act [Aug. 13, 2018], the Secretary of Defense shall create a list of countries that pose a risk to the cybersecurity of United States defense and national security systems and infrastructure. Such list shall reflect the level of threat posed by each country included on such list. In creating such list, the Secretary shall take in to account the following:

''(1) A foreign government's activities that pose force protection or cybersecurity risk to the personnel, financial systems, critical infrastructure, or information systems of the United States or coalition forces.

''(2) A foreign government's willingness and record of providing financing, logistics, training or intelligence to other persons, countries or entities posing a force protection or cybersecurity risk to the personnel, financial systems, critical infrastructure, or information systems of the United States or coalition forces.

''(3) A foreign government's engagement in foreign intelligence activities against the United States for the purpose of undermining United States national security.

''(4) A foreign government's knowing participation in transnational organized crime or criminal activity.

''(5) A foreign government's cyber activities and operations to affect the supply chain of the United States Government.

''(6) A foreign government's use of cyber means to unlawfully or inappropriately obtain intellectual property from the United States Government or United States persons.

''(b) UPDATES.—The Secretary shall continuously update and maintain the list under subsection (a) to preempt obsolescence.

''(c) REPORT TO CONGRESS.—Not later than one year after the date of the enactment of this Act, the Secretary shall submit to the appropriate committees of Congress the list created pursuant to subsection (a) and any accompanying analysis that contributed to the creation of the list.''

QUADRENNIAL COMPREHENSIVE CYBER POSTURE REVIEW

Pub. L. 115–91, div. A, title XVI, §1644, Dec. 12, 2017, 131 Stat. 1748, as amended by Pub. L. 116–92, div. A, title XVI, §1635, Dec. 20, 2019, 133 Stat. 1748; Pub. L. 116–283, div. A, title XVII, §1706, Jan. 1, 2021, 134 Stat. 4083, provided that:

''(a) REQUIREMENT FOR COMPREHENSIVE REVIEW.—In order to clarify the near-term policy and strategy of the United States with respect to cyber deterrence, the Secretary of Defense shall, not later than December 31, 2022, and quadrennially thereafter, conduct a comprehensive review of the cyber posture of the United States over the posture review period.

''(b) CONSULTATION.—The Secretary of Defense shall conduct each review under subsection (a) in consultation with the Director of National Intelligence, the Attorney General, the Secretary of Homeland Security, and the Secretary of State, as appropriate.

''(c) ELEMENTS OF REVIEW.—Each review conducted under subsection (a) shall include, for the posture review period, the following elements:

''(1) The assessment and definition of the role of cyber forces in the national defense and military strategies of the United States.

''(2) Review of the following:

''(A) The role of cyber operations in combatant commander warfighting plans.

''(B) The ability of combatant commanders to respond to adversary cyber attacks.

''(C) The international partner cyber capacity-building programs of the Department.

''(3) A review of the law, policies, and authorities relating to, and necessary for, the United States to maintain a safe, reliable, and credible cyber posture for defending against and responding to cyber attacks

and for deterrence in cyberspace, including the following:

''(A) An assessment of the need for further delegation of cyber-related authorities, including those germane to information warfare, to the Commander of United States Cyber Command.

''(B) An evaluation of the adequacy of mission authorities for all cyber-related military components, defense agencies, directorates, centers, and commands.

''(4) A review of the need for or for updates to a declaratory policy relating to the responses of the United States to cyber attacks of significant consequence.

''(5) A review of norms for the conduct of offensive cyber operations for deterrence and in crisis and conflict.

''(6) A review of a strategy to deter, degrade, or defeat malicious cyber activity targeting the United States (which may include activities, capability development, and operations other than cyber activities, cyber capability development, and cyber operations), including—

''(A) a review and assessment of various approaches to competition and deterrence in cyberspace, determined in consultation with experts from Government, academia, and industry;

''(B) a comparison of the strengths and weaknesses of the approaches identified pursuant to subparagraph (A) relative to the threat of each other; and

''(C) an assessment as to how the cyber strategy will inform country-specific campaign plans focused on key leadership of Russia, China, Iran, North Korea, and any other country the Secretary considers appropriate.

''(7) Identification of the steps that should be taken to bolster stability in cyberspace and, more broadly, stability between major powers, taking into account—

''(A) the analysis and gaming of escalation dynamics in various scenarios; and

''(B) consideration of the spiral escalatory effects of countries developing increasingly potent offensive cyber capabilities.

''(8) A comprehensive force structure assessment of the Cyber Operations Forces of the Department for the posture review period, including the following:

''(A) A determination of the appropriate size and composition of the Cyber Mission Forces to accomplish the mission requirements of the Department.

''(B) An assessment of the Cyber Mission Forces' personnel, capabilities, equipment, funding, operational concepts, and ability to execute cyber operations in a timely fashion.

''(C) An assessment of the personnel, capabilities, equipment, funding, and operational concepts of Cybersecurity Service Providers and other elements of the Cyber Operations Forces.

''(9) An assessment of whether the Cyber Mission Force has the appropriate level of interoperability, integration, and interdependence with special operations and conventional forces.

''(10) An evaluation of the adequacy of mission authorities for the Joint Force Provider and Joint Force Trainer responsibilities of United States Cyber Command, including the adequacy of the units designated as Cyber Operations Forces to support such responsibilities.

''(11) An assessment of the missions and resourcing of the combat support agencies in support of cyber missions of the Department.

''(12) An assessment of the potential costs, benefits, and value, if any, of establishing a cyber force as a separate uniformed service.

''(13) Any recurrent problems or capability gaps that remain unaddressed since the previous posture review.

''(14) Such other matters as the Secretary considers appropriate.

''(d) REPORT.—

''(1) IN GENERAL.—The Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the results of each cyber posture review conducted under subsection (a).

''(2) FORM OF REPORT.—Each report under paragraph (1) may be submitted in unclassified form or classified form, as necessary.

''(e) POSTURE REVIEW PERIOD DEFINED.—In this section, the term 'posture review period' means the eight-year period that begins on the date of each review conducted under subsection (a).''

§ 395. Notification requirements for sensitive military cyber operations

(a) IN GENERAL.—Except as provided in subsection (d), the Secretary of Defense shall promptly submit to the congressional defense committees notice in writing of any sensitive military cyber operation conducted under this title no later than 48 hours following such operation.

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

(2) The congressional defense committees shall ensure that committee procedures designed to protect from unauthorized disclosure classified information relating to national security of the United States are sufficient to protect the information that is submitted to the committees pursuant to this section.

(3) In the event of an unauthorized disclosure of a sensitive military cyber operation covered by this section, the Secretary shall ensure, to the maximum extent practicable, that the congressional defense committees are notified immediately of the sensitive military cyber operation concerned. The notification under this paragraph may be verbal or written, but in the event of a verbal notification a written notification, signed by the Secretary, or the Secretary's designee, shall be provided by not later than 48 hours after the provision of the verbal notification.

(c) SENSITIVE MILITARY CYBER OPERATION DEFINED.—(1) In this section, the term ''sensitive military cyber operation'' means an action described in paragraph (2) that—

(A) is carried out by the armed forces of the United States;

(B) is intended to achieve a cyber effect against a foreign terrorist organization or a country, including its armed forces and the proxy forces of that country located elsewhere—

(i) with which the armed forces of the United States are not involved in hostilities (as that term is used in section 4 of the War Powers Resolution (50 U.S.C. 1543)); or

(ii) with respect to which the involvement of the armed forces of the United States in hostilities has not been acknowledged publicly by the United States; and

(C)(i) is determined to—

(I) have a medium or high collateral effects estimate;

(II) have a medium or high intelligence gain or loss;

(III) have a medium or high probability of political retaliation, as determined by the political military assessment contained within the associated concept of operations;

(IV) have a medium or high probability of detection when detection is not intended; or

(V) result in medium or high collateral effects; or

(ii) is a matter the Secretary determines to be appropriate.

(2) The actions described in this paragraph are the following:

(A) An offensive cyber operation.

(B) A defensive cyber operation.

(d) EXCEPTIONS.—The notification requirement under subsection (a) does not apply—

(1) to a training exercise conducted with the consent of all nations where the intended effects of the exercise will occur; or

(2) to a covert action (as that term is defined in section 503 of the National Security Act of 1947 (50 U.S.C. 3093)).

(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide any new authority or to alter or otherwise affect the War Powers Resolution (50 U.S.C. 1541 et seq.), the Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note), or any requirement under the National Security Act of 1947 (50 U.S.C. 3001 et seq.).

(Added Pub. L. 115–91, div. A, title XVI, § 1631(a), Dec. 12, 2017, 131 Stat. 1736, § 130j; renumbered § 395 and amended Pub. L. 115–232, div. A, title X, § 1081(a)(1), title XVI, § 1631(a), Aug. 13, 2018, 132 Stat. 1983, 2123; Pub. L. 116–92, div. A, title XVI, § 1632, Dec. 20, 2019, 133 Stat. 1745; Pub. L. 116–283, div. A, title XVII, § 1702, Jan. 1, 2021, 134 Stat. 4080.)

Editorial Notes

REFERENCES IN TEXT

The War Powers Resolution, referred to in subsec. (e), is Pub. L. 93–148, Nov. 7, 1973, 87 Stat. 555, which is classified generally to chapter 33 (§ 1541 et seq.) of Title 50, War and National Defense. For complete classification of this Resolution to the Code, see Short Title note set out under section 1541 of Title 50 and Tables.

The Authorization for Use of Military Force, referred to in subsec. (e), is Pub. L. 107–40, Sept. 18, 2001, 115 Stat. 224, which is set out as a note under section 1541 of Title 50, War and National Defense.

The National Security Act of 1947, referred to in subsec. (e), is act July 26, 1947, ch. 343, 61 Stat. 495, which is classified principally to chapter 44 (§ 3001 et seq.) of Title 50, War and National Defense. For complete classification of this Act to the Code, see Tables.

AMENDMENTS

2021—Subsec. (c). Pub. L. 116–283 amended subsec. (c) generally. Prior to amendment, subsec. (c) defined ''sensitive military cyber operation'' as used in this section.

2019—Subsec. (b)(3). Pub. L. 116–92, § 1632(1), inserted '', signed by the Secretary, or the Secretary's designee,'' after ''written notification''.

Subsec. (c)(1)(B), (C). Pub. L. 116–92, § 1632(2)(A), added subpar. (B) and redesignated former subpar. (B) as (C).

Subsec. (c)(2)(B). Pub. L. 116–92, § 1632(2)(B), struck out ''outside the Department of Defense Information Networks to defeat an ongoing or imminent threat'' after ''A defensive cyber operation''.

2018—Pub. L. 115–232, § 1631(a), renumbered section 130j of this title as this section.

Subsec. (d)(2). Pub. L. 115–232, § 1081(a)(1), substituted ''section 503 of the National Security Act of 1947 (50 U.S.C. 3093)'' for ''section 3093 of title 50, United States Code''.

§ 396. Notification requirements for cyber weapons

(a) IN GENERAL.—Except as provided in subsection (c), the Secretary of Defense shall promptly submit to the congressional defense committees notice in writing of the following:

(1) With respect to a cyber capability that is intended for use as a weapon, on a quarterly basis, the aggregated results of all reviews of the capability for legality under international law pursuant to Department of Defense Directive 5000.01 carried out by any military department concerned.

(2) The use as a weapon of any cyber capability that has been approved for such use under international law by a military department no later than 48 hours following such use.

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

(2) The congressional defense committees shall ensure that committee procedures designed to protect from unauthorized disclosure classified information relating to national security of the United States are sufficient to protect the information that is submitted to the committees pursuant to this section.

(3) In the event of an unauthorized disclosure of a cyber capability covered by this section, the Secretary shall ensure, to the maximum extent practicable, that the congressional defense committees are notified immediately of the cyber capability concerned. The notification under this paragraph may be verbal or written, but in the event of a verbal notification a written notification shall be provided by not later than 48 hours after the provision of the verbal notification.

(c) EXCEPTIONS.—The notification requirement under subsection (a) does not apply—

(1) to a training exercise conducted with the consent of all nations where the intended effects of the exercise will occur; or

(2) to a covert action (as that term is defined in section 503 of the National Security Act of 1947 (50 U.S.C. 3093)).

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide any new authority or to alter or otherwise affect the War Powers Resolution (50 U.S.C. 1541 et seq.), the

Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note), or any requirement under the National Security Act of 1947 (50 U.S.C. 3001 et seq.).

(Added Pub. L. 115–91, div. A, title XVI, §1631(a), Dec. 12, 2017, 131 Stat. 1737, §130k; renumbered §396 and amended Pub. L. 115–232, div. A, title X, §1081(a)(1), title XVI, §1631(a), Aug. 13, 2018, 132 Stat. 1983, 2123.)

Editorial Notes

REFERENCES IN TEXT

The War Powers Resolution, referred to in subsec. (d), is Pub. L. 93–148, Nov. 7, 1973, 87 Stat. 555, which is classified generally to chapter 33 (§1541 et seq.) of Title 50, War and National Defense. For complete classification of this Resolution to the Code, see Short Title note set out under section 1541 of Title 50 and Tables.

The Authorization for Use of Military Force, referred to in subsec. (d), is Pub. L. 107–40, Sept. 18, 2001, 115 Stat. 224, which is set out as a note under section 1541 of Title 50, War and National Defense.

The National Security Act of 1947, referred to in subsec. (d), is act July 26, 1947, ch. 343, 61 Stat. 495, which is classified principally to chapter 44 (§3001 et seq.) of Title 50, War and National Defense. For complete classification of this Act to the Code, see Tables.

AMENDMENTS

2018—Pub. L. 115–232, §1631(a), renumbered section 130k of this title as this section.

Subsec. (c)(2). Pub. L. 115–232, §1081(a)(1), substituted ''section 503 of the National Security Act of 1947 (50 U.S.C. 3093)'' for ''section 3093 of title 50, United States Code''.

§397. Principal Information Operations Advisor

(a) DESIGNATION.—Not later than 30 days after the enactment of this Act, the Secretary of Defense shall designate, from among officials appointed to a position in the Department of Defense by and with the advice and consent of the Senate, a Principal Information Operations Advisor to act as the principal advisor to the Secretary on all aspects of information operations conducted by the Department.

(b) RESPONSIBILITIES.—The Principal Information Operations Advisor shall have the following responsibilities:

(1) Oversight of policy, strategy, planning, resource management, operational considerations, personnel, and technology development across all the elements of information operations of the Department.

(2) Overall integration and supervision of the deterrence of, conduct of, and defense against information operations.

(3) Promulgation of policies to ensure adequate coordination and deconfliction with the Department of State, the intelligence community (as such term is defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), and other relevant agencies and departments of the Federal Government.

(4) Coordination with the head of the Global Engagement Center to support the purpose of the Center (as set forth by section 1287(a)(2) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 22 U.S.C. 2656 note)) and liaison with the Center and other relevant Federal Government entities to support such purpose.

(5) Establishing and supervising a rigorous risk management process to mitigate the risk of potential exposure of United States persons to information intended exclusively for foreign audiences.

(6) Promulgation of standards for the attribution or public acknowledgment, if any, of operations in the information environment.

(7) Development of guidance for, and promotion of, the capability of the Department to liaison with the private sector and academia on matters relating to the influence activities of malign actors.

(8) Such other matters relating to information operations as the Secretary shall specify for purposes of this subsection.

(Added Pub. L. 116–92, div. A, title XVI, §1631(a)(1), Dec. 20, 2019, 133 Stat. 1741; amended Pub. L. 116–283, div. A, title X, §1081(a)(16), Jan. 1, 2021, 134 Stat. 3871.)

Editorial Notes

REFERENCES IN TEXT

The enactment of this Act, referred to in subsec. (a), probably means the date of enactment of Pub. L. 116–92, which added this section and was approved Dec. 20, 2019.

AMENDMENTS

2021—Subsec. (b)(5). Pub. L. 116–283 substituted ''persons'' for ''Persons''.

Statutory Notes and Related Subsidiaries

ASSESSMENT AND OPTIMIZATION OF DEPARTMENT OF DEFENSE INFORMATION AND INFLUENCE OPERATIONS CONDUCTED THROUGH CYBERSPACE

Pub. L. 117–263, div. A, title XV, §1522, Dec. 23, 2022, 136 Stat. 2897, provided that:

''(a) ASSESSMENT AND PLAN.—Not later than 90 days after the date of the enactment of this Act [Dec. 23, 2022], the Principal Information Operations Advisor and the Principal Cyber Advisor to the Secretary of Defense shall complete both an assessment and an optimization plan for information and influence operations conducted through cyberspace.

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

''(1) An inventory of the components of the Department of Defense conducting information and influence operations conducted through cyberspace.

''(2) An examination of sufficiency of resources allocated for information and influence operations conducted through cyberspace.

''(3) An evaluation of the command and control, oversight, and management of matters related to information and influence operations conducted through cyberspace across the Office of the Secretary of Defense and the Joint Staff.

''(4) An evaluation of the existing execution, coordination, synchronization, deconfliction, and consultative procedures and mechanisms for information and influence operations conducted through cyberspace.

''(5) Any other matters determined relevant by the Principal Information Operations Advisor and the Principal Cyber Advisor to the Secretary of Defense.

''(c) OPTIMIZATION PLAN.—The optimization plan under subsection (a) shall include the following:

''(1) Actions that the Department will implement to improve the execution, coordination, synchronization, deconfliction, and consultative procedures and mechanisms for information and influence operations conducted through cyberspace.

''(2) An evaluation of potential organizational changes required to optimize information and influence operations conducted through cyberspace.

''(3) Any other matters determined relevant by the Principal Information Operations Advisor and the Principal Cyber Advisor to the Secretary of Defense.

''(d) BRIEFINGS.—Not later than 30 days after completing the assessment and optimization plan under subsection (a), the Principal Information Operations Advisor and the Principal Cyber Advisor to the Secretary of Defense shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the assessment and plan.

''(e) IMPLEMENTATION.—Not later than 180 days after the date on which the briefing is provided under subsection (d), the Secretary of Defense shall implement the optimization plan under subsection (a).''

CONDUCTING OF MILITARY OPERATIONS IN THE INFORMATION ENVIRONMENT

Pub. L. 116–92, div. A, title XVI, §1631(b)–(i), Dec. 20, 2019, 133 Stat. 1742–1745, as amended by Pub. L. 116–283, div. A, title X, §1081(c)(6), title XVII, §1749(b), Jan. 1, 2021, 134 Stat. 3873, 4142, provided that:

''(b) AFFIRMING THE AUTHORITY OF THE SECRETARY OF DEFENSE TO CONDUCT MILITARY OPERATIONS IN THE INFORMATION ENVIRONMENT.—(1) Congress affirms that the Secretary of Defense is authorized to conduct military operations, including clandestine operations, in the information environment to defend the United States, allies of the United States, and interests of the United States, including in response to malicious influence activities carried out against the United States or a United States person by a foreign power.

''(2) The military operations referred to in paragraph (1), when appropriately authorized include the conduct of military operations short of hostilities and in areas outside of areas of active hostilities for the purpose of preparation of the environment, influence, force protection, and deterrence of hostilities.

''(c) TREATMENT OF CLANDESTINE MILITARY OPERATIONS IN THE INFORMATION ENVIRONMENT AS TRADITIONAL MILITARY ACTIVITIES.—A clandestine military operation in the information environment shall be considered a traditional military activity for the purposes of section 503(e)(2) of the National Security Act of 1947 (50 U.S.C. 3093(e)(2)).

''(d) QUARTERLY INFORMATION OPERATIONS BRIEFINGS.—(1) Not less frequently than once each quarter, 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 significant military operations, including all clandestine operations in the information environment, carried out by the Department of Defense during the immediately preceding quarter.

''(2) Each briefing under paragraph (1) shall include, with respect to the military operations in the information environment described in such paragraph, the following:

''(A) An update, disaggregated by geographic and functional command, that describes the operations carried out by the commands.

''(B) An overview of authorities and legal issues applicable to the operations, including any relevant legal limitations.

''(C) An outline of any interagency activities and initiatives relating to the operations.

''(D) Such other matters as the Secretary considers appropriate.

''(e) RULE OF CONSTRUCTION.—Nothing in this section may be construed to limit, expand, or otherwise alter the authority of the Secretary to conduct military operations, including clandestine operations, in the information environment, to authorize specific military operations, or to limit, expand, or otherwise alter or otherwise affect the War Powers Resolution (50 U.S.C. 1541 et seq.) or an authorization for use of military force that was in effect on the day before the date of the enactment of this Act [Dec. 20, 2019].

''(f) CROSS-FUNCTIONAL TEAM.—

''(1) ESTABLISHMENT.—The Principal Information Operations Advisor shall integrate the expertise in all elements of information operations and perspectives of appropriate organizations within the Office of the Secretary of Defense, Joint Staff, military departments, Defense Agencies, and combatant commands by establishing and maintaining a full-time cross-functional team composed of subject-matter experts selected from those organizations.

''(2) SELECTION AND ORGANIZATION.—The cross-functional team established under paragraph (1) shall be selected, organized, and managed in a manner consistent with section 911 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 10 U.S.C. 111 note).

''(g) STRATEGY AND POSTURE REVIEW.—

''(1) STRATEGY AND POSTURE REVIEW REQUIRED.—Not later than 270 days after the date of the enactment of this Act [Dec. 20, 2019], the Secretary of Defense, acting through the Principal Information Operations Advisor under section 397 of title 10, United States Code (as added by subsection (a)) and the cross-functional team established under subsection (f)(1), shall—

''(A) develop or update, as appropriate, a strategy for operations in the information environment, including how such operations will be synchronized across the Department of Defense and the global, regional, and functional interests of the combatant commands;

''(B) conduct an information operations posture review, including an analysis of capability gaps that inhibit the Department's ability to successfully execute the strategy developed or updated pursuant to subparagraph (A);

''(C) designate Information Operations Force Providers and Information Operations Joint Force Trainers for the Department of Defense;

''(D) develop and persistently manage a joint lexicon for terms related to information operations, including 'information operations', 'information environment', 'operations in the information environment', and 'information related capabilities'[;] and [sic]

''(E) determine the collective set of combat capabilities that will be treated as part of operations in the information environment, including cyber warfare, space warfare, military information support operations, electronic warfare, public affairs, and civil affairs; and

''(F) designate a Department of Defense entity to develop, apply, and continually refine an assessment capability for defining and measuring the impact of Department information operations, which entity shall be organizationally independent of Department components performing or otherwise engaged in operational support to Department information operations.

''(2) COORDINATION ON CERTAIN CYBER MATTERS.—For any matters in the strategy and posture review under paragraph (1) that involve or relate to Department of Defense cyber capabilities, the Principal Information Operations Advisor shall fully collaborate with the Principal Cyber Advisor to the Secretary of Defense.

''(3) ELEMENTS.—At a minimum, the strategy developed or updated pursuant to paragraph (1)(A) shall include the following:

''(A) The establishment of lines of effort, objectives, and tasks that are necessary to implement such strategy and eliminate the capability gaps identified under paragraph (1)(B).

''(B) In partnership with the Principal Cyber Advisor to the Secretary of Defense and in coordination with any other component or Department of Defense entity as selected by the Secretary of Defense, an evaluation of any organizational changes that may be required within the Office of the Secretary of Defense, including potential changes to Under Secretary or Assistant Secretary-level positions to comprehensively conduct oversight of policy development, capabilities, and other aspects of

operations in the information environment as determined pursuant to the information operations posture review under paragraph (1)(B).

''(C) An assessment of various models for operationalizing information operations, including the feasibility and advisability of establishing an Army Information Warfare Command.

''(D) A review of the role of information operations in combatant commander operational planning, the ability of combatant commanders to respond to hostile acts by adversaries, and the ability of combatant commanders to engage and build capacity with allies.

''(E) A review of the law, policies, and authorities relating to, and necessary for, the United States to conduct military operations, including clandestine military operations, in the information environment.

''(4) SUBMISSION TO CONGRESS.—Upon completion, the Secretary of Defense shall present the strategy for operations in the information environment and the information operations posture review under subparagraphs (A) and (B), respectively, of paragraph (1) to the Committees on Armed Services of the House of Representatives and the Senate.

''(h) REPORT.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act [Dec. 20, 2019], the Secretary of Defense shall provide the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives a report for the structuring and manning of information operations capabilities and forces across the Department of Defense. The Secretary shall provide such Committees with quarterly updates on such plan.

''(2) ELEMENTS.—The plan required under paragraph (1) shall address the following:

''(A) How the Department of Defense will organize to develop a combined information operations strategy and posture review under subsection (g).

''(B) How the Department will fulfill the roles and responsibilities of the Principal Information Operations Advisor under section 397 of title 10, United States Code (as added by subsection (a)).

''(C) How the Department will establish the information operations cross-functional team under subsection (f)(1).

''(D) How the Department will utilize boards and working groups involving senior-level Department representatives on information operations.

''(E) Such other matters as the Secretary of Defense considers appropriate.

''(i) DEFINITIONS.—In this section:

''(1) The terms 'foreign power' and 'United States person' have the meanings given such terms in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

''(2) The term 'hostilities' has the same meaning as such term is used in the War Powers Resolution (50 U.S.C. 1541 et seq.).

''(3) The term 'clandestine military operation in the information environment' means an operation or activity, or associated preparatory actions, authorized by the President or the Secretary of Defense, that—

''(A) is marked by, held in, or conducted with secrecy, where the intent is that the operation or activity will not be apparent or acknowledged publicly; and

''(B) is to be carried out—

''(i) as part of a military operation plan approved by the President or the Secretary of Defense;

''(ii) to deter, safeguard, or defend against attacks or malicious influence activities against the United States, allies of the United States, and interests of the United States;

''(iii) in support of hostilities or military operations involving the United States armed forces; or

''(iv) in support of military operations short of hostilities and in areas where hostilities are not occurring for the purpose of preparation of the environment, influence, force protection, and deterrence.''

[Amendment by Pub. L. 116–283, §1749(b), to section 1631(g) of Pub. L. 116–92, set out above, was executed to reflect the probable intent of Congress, notwithstanding errors in the directory language.]

[Pub. L. 116–283, div. A, title X, §1081(c), Jan. 1, 2021, 134 Stat. 3873, provided that the amendment made by section 1081(c)(6) of Pub. L. 116–283 to section 1631(i) of Pub. L. 116–92, set out above, is effective as of Dec. 20, 2020 (probably should be Dec. 20, 2019) and as if included in Pub. L. 116–92.]

§ 398. Military information support operations in information environment

(a) CONGRESSIONAL NOTIFICATION REQUIREMENT.—(1) Not later than 48 hours after the execution of any new military information support operation plan (in this section referred to as a ''MISO plan'') approved by the commander of a combatant command, or any change in scope of any existing MISO plan, including any underlying MISO supporting plan, the Secretary of Defense shall promptly submit to the congressional defense committees notice in writing of such approval or execution of change in scope.

(2) A notification under paragraph (1) with respect to a MISO plan shall include each of the following:

(A) A description of the military information support operation program (in this section referred to as a ''MISO program'') supported by the MISO plan.

(B) A description of the objectives of the MISO plan.

(C) A description of the intended target audience for military information support operation activities under the MISO plan.

(D) A description of the tactics, techniques, and procedures to be used in executing the MISO plan.

(E) A description of the personnel engaged in supporting or facilitating the operation.

(F) The amount of funding anticipated to be obligated and expended to execute the MISO plan during the current and subsequent fiscal years.

(G) The expected duration and desired outcome of the MISO plan.

(H) Any other elements the Secretary determines appropriate.

(3) To the maximum extent practicable, the Secretary shall ensure that the congressional defense committees are notified promptly of any unauthorized disclosure of a clandestine military support operation covered by this section. A notification under this subsection may be verbal or written, but in the event of a verbal notification, the Secretary shall provide a written notification by not later than 48 hours after the provision of the verbal notification.

(b) ANNUAL REPORT.—Not later than 90 days after the last day of any fiscal year during which the Secretary conducts a MISO plan, the Secretary shall submit to the congressional defense committees a report on all such MISO plans conducted during such fiscal year. Such report shall include each of the following:

(1) A list of each MISO program and the combatant command responsible for the program.

(2) For each MISO plan—

(A) a description of the plan and any supporting plans, including the objectives for the plan;

(B) a description of the intended target audience for the activities carried out under the plan and the means of distribution; and

(C) the cost of executing the plan.

(c) PROHIBITION ON CLANDESTINE OPERATIONS DESIGNED TO INFLUENCE OPINIONS AND POLITICS IN UNITED STATES.—None of the funds authorized to be appropriated or otherwise made available for the Department of Defense for any fiscal year may be used to conduct a clandestine military information support operation that is designed to influence—

(1) any political process taking place in the United States;

(2) the opinions of United States persons;

(3) United States policies; or

(4) media produced by United States entities for United States persons.

(Added Pub. L. 117–263, div. A, title X, § 1052(a), Dec. 23, 2022, 136 Stat. 2776.)

Editorial Notes

CODIFICATION

Another section 398 was renumbered section 398a of this title.

§ 398a. Pilot program for sharing cyber capabilities and related information with foreign operational partners

(a) AUTHORITY TO ESTABLISH PILOT PROGRAM TO SHARE CYBER CAPABILITIES.—The Secretary of Defense may, with the concurrence of the Secretary of State, provide cyber capabilities and related information developed or procured by the Department of Defense to foreign countries or organizations described in subsection (b) without compensation, to meet operational imperatives if the Secretary of Defense determines that the provision of such cyber capabilities is in the national security interests of the United States.

(b) LIST OF FOREIGN COUNTRIES.—The Secretary of Defense, with the concurrence of the Secretary of State, shall—

(1) establish—

(A) a list of foreign countries that the Secretary of Defense considers suitable for sharing of cyber capabilities and related information under the authority established under subsection (a); and

(B) criteria for establishing the list under subparagraph (A);

(2) not later than 14 days after establishing the list required by paragraph (1), submit to the appropriate committees of Congress such list; and

(3) notify the appropriate committees of Congress in writing of any changes to the list established under paragraph (1) at least 14 days prior to the adoption of any such changes.

(c) PROCEDURES.—Prior to the first use of the authority provided by subsection (a), the Secretaries of Defense and State shall—

(1) establish and submit to the appropriate committees of Congress procedures for a coordination process for subsection (a) that is consistent with the operational timelines required to support the national security of the United States; and

(2) notify the appropriate committees of Congress in writing of any changes to the procedures established under paragraph (1) at least 14 days prior to the adoption of any such changes.

(d) NOTIFICATION REQUIRED.—(1) The Secretary of Defense and Secretary of State jointly shall promptly submit to the appropriate committees of Congress notice in writing of any use of the authority provided by subsection (a) no later than 48 hours following the use of the authority.

(2) Notification under paragraph (1) shall include a certification that the provision of the cyber capabilities was in the national security interests of the United States.

(3) The notification under paragraph (1) shall include an analysis of whether the transfer and the underlying operational imperative could have been met using another authority.

(e) TERMINATION.—The authority established under subsection (a) shall terminate on the date that is 3 years after the date on which this authority becomes law.

(f) PERFORMANCE METRICS.—(1) The Secretary of Defense shall maintain performance metrics to track the results of sharing cyber capabilities and related information with foreign operational partners under a pilot program authorized by subsection (a).

(2) The performance metrics under paragraph (1) shall include the following:

(A) Whom the cyber capability was used against.

(B) The effect of the cyber capability, including whether and how the transfer of the cyber capability improved the operational cyber posture of the United States and achieved operational objectives of the United States, or had no effect.

(C) Such other outcome-based or appropriate performance metrics as the Secretary considers appropriate for evaluating the effectiveness of a pilot program carried out under subsection (a).

(g) DEFINITIONS.—In this section:

(1) The term ''appropriate committees of Congress'' means—

(A) the congressional defense committees;

(B) the Committee on Foreign Relations of the Senate; and

(C) Committee on Foreign Affairs of the House of Representatives.

(2) The term ''cyber capability'' means a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.

(h) RULE OF CONSTRUCTION.—Nothing in this section shall be construed as amending, diminishing, or otherwise impacting reporting or other obligations under the War Powers Resolution.

(Added Pub. L. 117–263, div. A, title XV, § 1551(a), Dec. 23, 2022, 136 Stat. 2918, § 398; renumbered

§ 398a and amended Pub. L. 118–31, div. A, title XV, § 1501, title XVIII, § 1801(a)(6), (7), Dec. 22, 2023, 137 Stat. 533, 683.)

Editorial Notes

REFERENCES IN TEXT

The War Powers Resolution, referred to in subsec. (h), is Pub. L. 93–148, Nov. 7, 1973, 87 Stat. 555, which is classified generally to chapter 33 (§ 1541 et seq.) of Title 50, War and National Defense. For complete classification of this Resolution to the Code, see Short Title note set out under section 1541 of Title 50 and Tables.

AMENDMENTS

2023—Pub. L. 118–31, §§ 1501(1), 1801(a)(6), made identical amendments, renumbering section 398 of this title relating to pilot program for sharing cyber capabilities and related information with foreign operational partners as this section.

Subsec. (b)(1)(A). Pub. L. 118–31, § 1801(a)(7)(A)(i), substituted ''subsection (a)'' for ''paragraph (a)''.

Subsec. (b)(2). Pub. L. 118–31, § 1801(a)(7)(A)(ii), substituted ''paragraph (1)'' for ''paragraph (a)''.

Subsec. (b)(3). Pub. L. 118–31, § 1801(a)(7)(A)(iii), substituted ''paragraph (1)'' for ''clause (1)''.

Subsec. (e). Pub. L. 118–31, § 1801(a)(7)(B), substituted ''subsection (a)'' for ''paragraph (a)''.

Subsecs. (f) to (h). Pub. L. 118–31, § 1501(2), added subsec. (f) and redesignated former subsecs. (f) and (g) as (g) and (h), respectively.

§ 399. Notifications relating to military operations in the information environment: requirement to notify Chief of Mission

The Secretary may not authorize a military operation in the information environment under this title intended to cause an effect in a country unless the Secretary fully informs the chief of mission for that country under section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927) of the planned operation.

(Added Pub. L. 117–263, div. A, title XV, § 1521, Dec. 23, 2022, 136 Stat. 2897.)

CHAPTER 20—HUMANITARIAN AND OTHER ASSISTANCE

Sec.

Editorial Notes

PRIOR PROVISIONS

Chapter was comprised of subchapter I, sections 401 to 404, and subchapter II, section 410, prior to amendment by Pub. L. 104–106, div. A, title V, § 571(c), Feb. 10, 1996, 110 Stat. 353, which struck out headings for subchapters I and II.

AMENDMENTS

2023—Pub. L. 118–31, div. A, title X, § 1042(a)(1), Dec. 22, 2023, 137 Stat. 388, substituted ''Assistance in support of'' for ''Equipment and training of foreign personnel to assist in'' in item 408. Amendment was made pursuant to operation of section 102 of this title.

2011—Pub. L. 112–81, div. A, title X, § 1092(b)(2), Dec. 31, 2011, 125 Stat. 1606, added item 407 and struck out former item 407 ''Humanitarian demining assistance: authority; limitations''.

2008—Pub. L. 110–417, [div. A], title X, § 1031(b), Oct. 14, 2008, 122 Stat. 4590, added item 409.

Pub. L. 110–181, div. A, title XII, § 1207(b), Jan. 28, 2008, 122 Stat. 367, added item 408.

2006—Pub. L. 109–364, div. A, title XII, § 1203(b)(2), Oct. 17, 2006, 120 Stat. 2415, added item 407.

1996—Pub. L. 104–106, div. A, title X, § 1061(g)(2), title XIII, § 1301(b), Feb. 10, 1996, 110 Stat. 443, 473, which directed amendment of table of sections at beginning of subchapter I of this chapter by striking out item 403 and adding item 405, were executed by striking out item 403 ''International peacekeeping activities'' and adding item 405 in analysis for this chapter to reflect the probable intent of Congress and amendments by Pub. L. 104–106, § 571(c)(1), (2). See below.

Pub. L. 104–106, div. A, title V, § 571(c)(1), (2), Feb. 10, 1996, 110 Stat. 353, struck out subchapter analysis, consisting of items for subchapter I ''Humanitarian Assistance'' and subchapter II ''Civil-Military Cooperation'' and struck out subchapter I heading ''HUMANITARIAN ASSISTANCE''.

1994—Pub. L. 103–337, div. A, title XIV, § 1412(b), Oct. 5, 1994, 108 Stat. 2913, added item 404.

1992—Pub. L. 102–484, div. A, title X, § 1081(b)(2), title XIII, § 1342(c)(2), Oct. 23, 1992, 106 Stat. 2516, 2558, added subchapter analysis, subchapter I heading, and item 403.

1987—Pub. L. 100–180, div. A, title III, § 332(b)(6), Dec. 4, 1987, 101 Stat. 1080, substituted ''HUMANITARIAN AND OTHER ASSISTANCE'' for ''HUMANITARIAN AND CIVIC ASSISTANCE PROVIDED IN CONJUNCTION WITH MILITARY OPERATIONS'' in chapter heading, ''Humanitarian and civic assistance provided in conjunction with military operations'' for ''Armed forces participation in humanitarian and civic assistance activities'' in item 401, and ''Transportation of humanitarian relief supplies to foreign countries'' for ''Approval of Secretary of State'' in item 402, and struck out items 403 ''Payment of expenses'', 404 ''Annual report to Congress'', 405 ''Definition of humanitarian and civic assistance'', and 406 ''Expenditure limitation''.

§ 401. Humanitarian and civic assistance provided in conjunction with military operations

(a)(1) Under regulations prescribed by the Secretary of Defense, the Secretary of a military department may carry out humanitarian and civic assistance activities in conjunction with authorized military operations of the armed forces in a country if the Secretary concerned determines that the activities will promote—

(A) the security interests of both the United States and the country in which the activities are to be carried out; and

(B) the specific operational readiness skills of the members of the armed forces who participate in the activities.

(2) Humanitarian and civic assistance activities carried out under this section shall complement, and may not duplicate, any other form of social or economic assistance which may be provided to the country concerned by any other department or agency of the United States. Such activities shall serve the basic economic