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.