(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.