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