

“(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.”

§ 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 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; and

(B) is intended to cause cyber effects outside a geographic location—

(i) where the armed forces of the United States are involved in hostilities (as that term is used in section 1543 of title 50, United States Code); or

(ii) with respect to which hostilities have been declared by the United States.

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

(A) An offensive cyber operation.

(B) A defensive cyber operation outside the Department of Defense Information Networks to defeat an ongoing or imminent threat.

(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.)

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

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.)

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”.

CHAPTER 20—HUMANITARIAN AND OTHER ASSISTANCE

Sec.	
401.	Humanitarian and civic assistance provided in conjunction with military operations.
402.	Transportation of humanitarian relief supplies to foreign countries.
[403.	Repealed.]
404.	Foreign disaster assistance.
405.	Use of Department of Defense funds for United States share of costs of United Nations peacekeeping activities: limitation.
[406.	Renumbered.]
407.	Humanitarian demining assistance and stockpiled conventional munitions assistance: authority; limitations.
408.	Equipment and training of foreign personnel to assist in Department of Defense accounting for missing United States Government personnel.
409.	Center for Complex Operations.
[410.	Repealed.]

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.