(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.)

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.''

§ 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, Technology, and Logistics.

(C) The Under Secretary of Defense for Intelligence.

(D) The Chief Information Officer of the Department of Defense.

(E) 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.)

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

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.)

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 military 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.

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 at-