(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.''

CHAPTER 20—HUMANITARIAN AND OTHER ASSISTANCE

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.

AMENDMENTS

2011—Pub. L. 112–81, div. A, title X, § 1092(b)(2), Dec. 31, 2011, 125 Stat. 1606, added item 407 and struck out former item 407 ''Humanitarian demining assistance: authority; limitations''.

2008—Pub. L. 110–417, [div. A], title X, § 1031(b), Oct. 14, 2008, 122 Stat. 4590, added item 409.

Pub. L. 110–181, div. A, title XII, § 1207(b), Jan. 28, 2008, 122 Stat. 367, added item 408.

2006—Pub. L. 109–364, div. A, title XII, § 1203(b)(2), Oct. 17, 2006, 120 Stat. 2415, added item 407.