that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

(Added Pub. L. 113–291, div. A, title XVI, §1632(a), Dec. 19, 2014, 128 Stat. 3639; amended Pub. L. 114–92, div. A, title XVI, §1641(b), (c)(1), Nov. 25, 2015, 129 Stat. 1115, 1116.)

AMENDMENTS

2015—Subsec. (a). Pub. L. 114–92, §1641(c)(1), substituted ''and section 393 of this title'' for ''and with section 941 of the National Defense Authorization Act for Fiscal Year 2013 (10 U.S.C. 2224 note)''.

Subsecs. (d), (e). Pub. L. 114–92, §1641(b), added subsec. (d) and redesignated former subsec. (d) as (e).

ISSUANCE OF PROCEDURES

Pub. L. 113–291, div. A, title XVI, §1632(b), Dec. 19, 2014, 128 Stat. 3640, provided that: ''The Secretary shall establish the procedures required by subsection (b) of section 391 of title 10, United States Code, as added by subsection (a) of this section, not later than 90 days after the date of the enactment of this Act [Dec. 19, 2014].''

ASSESSMENT OF DEPARTMENT POLICIES

Pub. L. 113–291, div. A, title XVI, §1632(c), Dec. 19, 2014, 128 Stat. 3640, provided that:

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of the Act [Dec. 19, 2014], the Secretary of Defense shall complete an assessment of—

''(A) requirements that were in effect on the day before the date of the enactment of this Act for contractors to share information with Department components regarding cyber incidents (as defined in subsection (d) of such section 391 [10 U.S.C. 391]) with respect to networks or information systems of contractors; and

''(B) Department policies and systems for sharing information on cyber incidents with respect to networks or information systems of Department contractors.

''(2) ACTIONS FOLLOWING ASSESSMENT.—Upon completion of the assessment required by paragraph (1), the Secretary shall—

''(A) designate a Department component under subsection (a) of such section 391; and

''(B) issue or revise guidance applicable to Department components that ensures the rapid sharing by the component designated pursuant to such section 391 or section 941 of the National Defense Authorization Act for Fiscal Year 2013 [Pub. L. 112–239] (10 U.S.C. 2224 note) of information relating to cyber incidents with respect to networks or information systems of contractors with other appropriate Department components.''

§ 392. Executive agents for cyber test and training ranges

(a) EXECUTIVE AGENT.—The Secretary of Defense, in consultation with the Principal Cyber Advisor, shall—

(1) designate a senior official from among the personnel of the Department of Defense to act as the executive agent for cyber and information technology test ranges; and

(2) designate a senior official from among the personnel of the Department of Defense to act as the executive agent for cyber and information technology training ranges.

(b) ROLES, RESPONSIBILITIES, AND AUTHORITIES.—

(1) ESTABLISHMENT.—The Secretary of Defense shall prescribe the roles, responsibilities, and authorities of the executive agents designated under subsection (a). Such roles, responsibilities, and authorities shall include the development of a biennial integrated plan for cyber and information technology test and training resources.

(2) BIENNIAL INTEGRATED PLAN.—The biennial integrated plan required under paragraph (1) shall include plans for the following:

(A) Developing and maintaining a comprehensive list of cyber and information technology ranges, test facilities, test beds, and other means of testing, training, and developing software, personnel, and tools for accommodating the mission of the Department. Such list shall include resources from both governmental and nongovernmental entities.

(B) Organizing and managing designated cyber and information technology test ranges, including—

(i) establishing the priorities for cyber and information technology ranges to meet Department objectives;

(ii) enforcing standards to meet requirements specified by the United States Cyber Command, the training community, and the research, development, testing, and evaluation community;

(iii) identifying and offering guidance on the opportunities for integration amongst the designated cyber and information technology ranges regarding test, training, and development functions;

(iv) finding opportunities for cost reduction, integration, and coordination improvements for the appropriate cyber and information technology ranges;

(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)