the Secretary with respect to the review conducted by the Secretary pursuant to paragraph (1).''

CONSORTIA OF UNIVERSITIES TO ADVISE SECRETARY OF DEFENSE ON CYBERSECURITY MATTERS

Pub. L. 116–92, div. A, title XVI, § 1659, Dec. 20, 2019, 133 Stat. 1770, provided that:

''(a) ESTABLISHMENT AND FUNCTION.—The Secretary of Defense shall establish one or more consortia of universities to assist the Secretary on cybersecurity matters relating to the following:

''(1) To provide the Secretary a formal mechanism to communicate with consortium or consortia members regarding the Department of Defense's cybersecurity strategic plans, cybersecurity requirements, and priorities for basic and applied cybersecurity research.

''(2) To advise the Secretary on the needs of academic institutions related to cybersecurity and research conducted on behalf of the Department and provide feedback to the Secretary from members of the consortium or consortia.

''(3) To serve as a focal point or focal points for the Secretary and the Department for the academic community on matters related to cybersecurity, cybersecurity research, conceptual and academic developments in cybersecurity, and opportunities for closer collaboration between academia and the Department.

''(4) To provide to the Secretary access to the expertise of the institutions of the consortium or consortia on matters relating to cybersecurity.

''(5) To align the efforts of such members in support of the Department.

''(b) MEMBERSHIP.—The consortium or consortia established under subsection (a) shall be open to all universities that have been designated as centers of academic excellence by the Director of the National Security Agency or the Secretary of Homeland Security.

''(c) ORGANIZATION.—

''(1) DESIGNATION OF ADMINISTRATIVE CHAIR AND TERMS.—For each consortium established under subsection (a), the Secretary of Defense, based on recommendations from the members of the consortium, shall designate one member of the consortium to function as an administrative chair of the consortium for a term with a specific duration specified by the Secretary.

''(2) SUBSEQUENT TERMS.—No member of a consortium designated under paragraph (1) may serve as the administrative chair of that consortium for two consecutive terms.

''(3) DUTIES OF ADMINISTRATIVE CHAIR.—Each administrative chair designated under paragraph (1) for a consortium shall—

''(A) act as the leader of the consortium for the term specified by the Secretary under paragraph (1);

''(B) be the liaison between the consortium and the Secretary;

''(C) distribute requests from the Secretary for advice and assistance to appropriate members of the consortium and coordinate responses back to the Secretary; and

''(D) act as a clearinghouse for Department of Defense requests relating to assistance on matters relating to cybersecurity and to provide feedback to the Secretary from members of the consortium.

''(4) EXECUTIVE COMMITTEE.—For each consortium, the Secretary, in consultation with the administrative chair, may form an executive committee comprised of university representatives to assist the chair with the management and functions of the consortia. Executive committee institutions may not serve consecutive terms before all other consortium institutions have been afforded the opportunity to hold the position.

''(d) CONSULTATION.—The Secretary, or a senior level designee, shall meet with each consortium not less frequently than twice per year, or at a periodicity agreed to between the Department and each such consortium.

''(e) PROCEDURES.—The Secretary shall establish procedures for organizations within the Department to access the work product produced by and the research, capabilities, and expertise of a consortium established under subsection (a) and the universities that constitute such consortium.''

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) [now (e)] of such section 391 [10 U.S.C. 391(e)]) 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