provide to the Committees on Armed Services of the Senate and the House of Representatives a briefing on the findings from the report on enhancing training and coordination to advance cyberspace security cooperation described in such subsection. Such briefing shall include a discussion on the enhanced training meeting the elements under subsection (a)(3) and a plan for future updates and sustainment of such training.''

§ 391. Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors

(a) DESIGNATION OF DEPARTMENT COMPONENT TO RECEIVE REPORTS.—The Secretary of Defense shall designate a component of the Department of Defense to receive reports of cyber incidents from contractors in accordance with this section and section 393 of this title or from other governmental entities.

(b) PROCEDURES FOR REPORTING CYBER INCIDENTS.—The Secretary of Defense shall establish procedures that require an operationally critical contractor to report in a timely manner to component designated under subsection (a) each time a cyber incident occurs with respect to a network or information system of such operationally critical contractor.

(c) PROCEDURE REQUIREMENTS.—

(1) DESIGNATION AND NOTIFICATION.—The procedures established pursuant to subsection (a) shall include a process for—

(A) designating operationally critical contractors; and

(B) notifying a contractor that it has been designated as an operationally critical contractor.

(2) RAPID REPORTING.—The procedures established pursuant to subsection (a) shall require each operationally critical contractor to rapidly report to the component of the Department designated pursuant to subsection (d)(2)(A) on each cyber incident with respect to any network or information systems of such contractor. Each such report shall include the following:

(A) An assessment by the contractor of the effect of the cyber incident on the ability of the contractor to meet the contractual requirements of the Department.

(B) The technique or method used in such cyber incident.

(C) A sample of any malicious software, if discovered and isolated by the contractor, involved in such cyber incident.

(D) A summary of information compromised by such cyber incident.

(3) DEPARTMENT ASSISTANCE AND ACCESS TO EQUIPMENT AND INFORMATION BY DEPARTMENT PERSONNEL.—The procedures established pursuant to subsection (a) shall—

(A) include mechanisms for Department personnel to, if requested, assist operationally critical contractors in detecting and mitigating penetrations; and

(B) provide that an operationally critical 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.

(4) PROTECTION OF TRADE SECRETS AND OTHER INFORMATION.—The procedures established pursuant to subsection (a) shall provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person.

(5) DISSEMINATION OF INFORMATION.—The procedures established pursuant to subsection (a) shall limit the dissemination of information obtained or derived through the 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 OPERATIONALLY CRITICAL CONTRACTORS.—(1) No cause of action shall lie or be maintained in any court against any operationally critical contractor, and such action shall be promptly dismissed, for compliance with this section and contract requirements established pursuant to Defense Federal Acquisition Regulation Supplement clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, that is conducted in accordance with procedures established pursuant to subsection (b) and such contract requirements.

(2)(A) Nothing in this section shall be construed—

(i) to require dismissal of a cause of action against an operationally critical contractor that has engaged in willful misconduct in the course of complying with the procedures established pursuant to subsection (b); 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 operationally critical 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) CYBER INCIDENT.—The term ''cyber incident'' means actions taken through the use of

computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

(2) OPERATIONALLY CRITICAL CONTRACTOR.—The term ''operationally critical contractor'' means a contractor designated by the Secretary for purposes of this section as a critical source of supply for airlift, sealift, intermodal transportation services, or logistical support 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; Pub. L. 116–283, div. A, title XVII, §1704, Jan. 1, 2021, 134 Stat. 4082.)

Editorial Notes

AMENDMENTS

2021—Subsec. (d)(1). Pub. L. 116–283 inserted ''and contract requirements established pursuant to Defense Federal Acquisition Regulation Supplement clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting,'' after ''compliance with this section'' and ''and such contract requirements'' before period at end.

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).

Statutory Notes and Related Subsidiaries

SENIOR MILITARY ADVISOR FOR CYBER POLICY AND DEPUTY PRINCIPAL CYBER ADVISOR

Pub. L. 116–92, div. A, title IX, §905, Dec. 20, 2019, 133 Stat. 1557, as amended by Pub. L. 116–283, div. A, title XVII, §1713(b), Jan. 1, 2021, 134 Stat. 4090; Pub. L. 117–81, div. A, title XV, §1503(b), Dec. 27, 2021, 135 Stat. 2021; Pub. L. 117–263, div. A, title X, §1081(c), Dec. 23, 2022, 136 Stat. 2797, which authorized the Secretary of Defense to designate an officer within the Office of the Under Secretary of Defense for Policy to serve within that Office as Senior Military Advisor for Cyber Policy, and concurrently, as Deputy Principal Cyber Advisor, was transferred to section 392a of this chapter and designated as subsec. (b) of that section by Pub. L. 117–263, div. A, title XV, §1501(b)(3)(A), Dec. 23, 2022, 136 Stat. 2878.

CYBER GOVERNANCE STRUCTURES AND PRINCIPAL CYBER ADVISORS ON MILITARY CYBER FORCE MATTERS

Pub. L. 116–92, div. A, title XVI, §1657, Dec. 20, 2019, 133 Stat. 1767, which authorized each of the secretaries of the military departments, in consultation with the service chiefs, to appoint an independent Principal Cyber Advisor for each service to act as the principal advisor to the relevant secretary on all cyber matters affecting that military service, was transferred to section 392a of this chapter and designated as subsec. (c) of that section by Pub. L. 117–263, div. A, title XV, §1501(b)(4)(A), Dec. 23, 2022, 136 Stat. 2878.

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, as amended by Pub. L. 117–81, div. A, title XV, §1530, Dec. 27, 2021, 135 Stat. 2049; Pub. L. 117–263, div. A, title XV, §1505, Dec. 23, 2022, 136 Stat. 2881; Pub. L. 118–31, div. A, title XV, §1531(c)(3), Dec. 22, 2023, 137 Stat. 562, provided that:

''(a) ESTABLISHMENT AND FUNCTION.—The Secretary of Defense shall establish a consortium 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 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 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.—The Secretary of Defense shall designate the National Defense University College of Information and Cyberspace to function as the administrative chair of the consortium established pursuant to subsection (a).

''(2) DUTIES OF ADMINISTRATIVE CHAIR.—The administrative chair designated under paragraph (1) for the consortium shall—

''(A) act as the leader of the consortium;

''(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.

''(3) EXECUTIVE COMMITTEE.—The Secretary, in consultation with the administrative chair, may form an executive committee for the consortium that is comprised of representatives of the Federal Government to assist the chair with the management and functions of the consortium.

''(d) CONSULTATION.—The Secretary shall meet with such members of the consortium as the Secretary considers appropriate, not less frequently than twice each year or at such periodicity as is agreed to by the Secretary and the 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.

''(f) SUPPORT CENTER.—

''(1) ESTABLISHMENT.—The Secretary shall establish a center to provide support to the consortium established under subsection (a).

''(2) COMPOSITION.—

''(A) REQUIREMENT.—The center established under paragraph (1) shall be composed of one or two universities, as the Secretary considers appropriate, that—

''(i) have been designated as centers of academic excellence by the Director of the National Security Agency or the Secretary of Homeland Security; and

''(ii) are eligible for access to classified information.

''(B) PUBLICATION.—The Secretary shall publish in the Federal Register the process for selection of universities to serve as the center established under paragraph (1).

''(3) FUNCTIONS.—The functions of the center established under paragraph (1) are as follows:

''(A) To promote the consortium established under subsection (a).

''(B) To distribute on behalf of the Department requests for information or assistance to members of the consortium.

''(C) To collect and assemble responses from requests distributed under subparagraph (B).

''(D) To provide additional administrative support for the consortium.

''(g) DISCHARGE THROUGH DIRECTOR.—In carrying out this section, the Secretary of Defense shall act through the Director of the office established under section 2192c of title 10, United States Code.''

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.''

§ 391a. Annual reports on support by military departments for United States Cyber Command

(a) REPORTS.—Not later than 15 days after the date on which the Secretary of Defense submits to Congress the defense budget materials (as defined in section 239 of this title) for a fiscal year, the Commander of the United States Cyber Command shall submit to the congressional defense committees a report containing the following:

(1) An evaluation of whether each military department is meeting the requirements established by the Commander and validated by the Office of the Secretary of Defense, and is effectively implementing the plan required by section 1534 of the National Defense Authorization Act for Fiscal Year 2023, and the requirements established pursuant to section 1533 of such Act.

(2) For each military department evaluated under paragraph (1)—

(A) a certification that the military department is meeting such requirements; or

(B) a detailed explanation regarding how the military department is not meeting such requirements.

(b) ELEMENTS OF EVALUATION.—Each evaluation under subsection (a)(1) shall include, with respect to the military department being evaluated, the following:

(1) The adequacy of the policies, procedures, and execution of manning, training, and equipping personnel for employment within the Cyber Mission Force.

(2) The sufficiency and robustness of training curricula for personnel to be assigned to either the Cyber Mission Force or units within the cyberspace operations forces, and the compliance by the military department with training standards.

(3) The adequacy of the policies and procedures relating to the assignment and assignment length of members of the Army, Navy, Air Force, Marine Corps, or Space Force to the Cyber Mission Force.

(4) The efficacy of the military department in filling key work roles within the Cyber Mission Force, including the proper force mix of civilian, military, and contractor personnel, and the means necessary to meet requirements established by the Commander and validated by the Secretary of Defense.

(5) The adequacy of the investment to advance cyber-peculiar science and technology, particularly with respect to capability development for the Cyber Mission Force.

(6) The sufficiency of the policies, procedures, and investments relating to the establishment and management of military occupational specialty, designator, rating, or Air Force specialty code for personnel responsible for cyberspace operations, including an assessment of the effectiveness of the combination of policies determining availability and retention of sufficient numbers of proficient personnel in key work roles, including length of service commitment, the use of bonuses and special pays, alternative compensation mechanisms, and consecutive tours in preferred assignments.

(7) In coordination with the Principal Cyber Advisor of the Department of Defense, an evaluation of the use by the military department of the shared lexicon of the Department of Defense specific to cyberspace activities.

(8) The readiness of personnel serving in the Cyber Mission Force and the cyberspace operations forces to accomplish assigned missions.

(9) The adequacy of actions taken during the period of evaluation by the military department to respond to findings from any previous years' evaluations.

(10) Any other element determined relevant by the Commander.

(Added Pub. L. 117–263, div. A, title XV, §1502(a), Dec. 23, 2022, 136 Stat. 2879.)