INFORMATION OPERATIONS MATTERS'' for ''CYBER MATTERS'' in chapter heading and added item 397.

2018—Pub. L. 115–232, div. A, title XVI, §1631(c)(2), Aug. 13, 2018, 132 Stat. 2123, added items 394 to 396.

2015—Pub. L. 114–92, div. A, title X, §1081(a)(4), title XVI, §1641(c)(2), Nov. 25, 2015, 129 Stat. 1001, 1116, substituted ''Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors'' for ''Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors'' in item 391 and added item 393.

2014—Pub. L. 113–291, div. A, title XVI, §1633(d), Dec. 19, 2014, 128 Stat. 3643, added item 392.

§ 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.)

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).

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, provided that:

''(a) ADVISOR.—

''(1) IN GENERAL.—The Secretary of Defense shall, acting through the Joint Staff, designate an officer within the Office of the Secretary of Defense to serve within that Office as the Senior Military Advisor for Cyber Policy, and concurrently, as the Deputy Principal Cyber Advisor.

''(2) OFFICERS ELIGIBLE FOR DESIGNATION.—The officer designated pursuant to this subsection shall be designated from among commissioned regular officers of the Armed Forces in a general or flag officer grade who are qualified for designation[.]

''(3) GRADE.—The officer designated pursuant to this subsection shall have the grade of major general or rear admiral (upper half) while serving in that position, without vacating the officer's permanent grade.

''(b) SCOPE OF POSITIONS.—

''(1) IN GENERAL.—The officer designated pursuant to subsection (a) is each of the following:

''(A) The Senior Military Advisor for Cyber Policy to the Under Secretary of Defense for Policy.

''(B) The Deputy Principal Cyber Advisor to the Secretary of Defense.

''(2) DIRECTION AND CONTROL AND REPORTING.—In carrying out duties under this section, the officer designed [sic, probably should be ''designated''] pursuant to subsection (a) shall be subject to the authority, direction, and control of, and shall report directly to, the following:

''(A) The Under Secretary with respect to Senior Military Advisor for Cyber Policy duties.

''(B) The Principal Cyber Advisor with respect to Deputy Principal Cyber Advisor duties.

''(c) DUTIES.—

''(1) DUTIES AS SENIOR MILITARY ADVISOR FOR CYBER POLICY.—The duties of the officer designated pursuant to subsection (a) as Senior Military Advisor for Cyber Policy are as follows:

''(A) To serve as the principal uniformed military advisor on military cyber forces and activities to the Under Secretary of Defense for Policy.

''(B) To assess and advise the Under Secretary on aspects of policy relating to military cyberspace operations, resources, personnel, cyber force readiness, cyber workforce development, and defense of Department of Defense networks.

''(C) To advocate, in consultation with the Joint Staff, and senior officers of the Armed Forces and the combatant commands, for consideration of military issues within the Office of the Under Secretary of Defense for Policy, including coordination and synchronization of Department cyber forces and activities.

''(D) To maintain open lines of communication between the Chief Information Officer of the Department of Defense, senior civilian leaders within the Office of the Under Secretary, and senior officers on the Joint Staff, the Armed Forces, and the combatant commands on cyber matters, and to ensure that military leaders are informed on cyber policy decisions.

''(2) DUTIES AS DEPUTY PRINCIPAL CYBER ADVISOR.—The duties of the officer designated pursuant to subsection (a) as Deputy Principal Cyber Advisor are as follows:

''(A) To synchronize, coordinate, and oversee implementation of the Cyber Strategy of the Department of Defense and other relevant policy and planning.

''(B) To advise the Secretary of Defense on cyber programs, projects, and activities of the Department, including with respect to policy, training, resources, personnel, manpower, and acquisitions and technology.

''(C) To oversee implementation of Department policy and operational directives on cyber programs, projects, and activities, including with respect to resources, personnel, manpower, and acquisitions and technology.

''(D) To assist in the overall supervision of Department cyber activities relating to offensive missions.

''(E) To assist in the overall supervision of Department defensive cyber operations, including activities of component-level cybersecurity service providers and the integration of such activities with activities of the Cyber Mission Force.

''(F) To advise senior leadership of the Department on, and advocate for, investment in capabilities to execute Department missions in and through cyberspace.

''(G) To identify shortfalls in capabilities to conduct Department missions in and through cyberspace, and make recommendations on addressing such shortfalls in the Program Budget Review process.

''(H) To coordinate and consult with stakeholders in the cyberspace domain across the Department in order to identify other issues on cyberspace for the attention of senior leadership of the Department.

''(I) On behalf of the Principal Cyber Advisor, to lead the cross-functional team established pursuant to 932(c)(3) of the National Defense Authorization Act for Fiscal Year 2014 [Pub. L. 113–66] (10 U.S.C. 2224 note) in order to synchronize and coordinate military and civilian cyber forces and activities of the Department.''

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, provided that:

''(a) DESIGNATION.—

''(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act [Dec. 20, 2019], each of the secretaries of the military departments, in consultation with the service chiefs, shall 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.

''(2) NATURE OF POSITION.—Each Principal Cyber Advisor position under paragraph (1) shall—

''(A) be a senior civilian leadership position, filled by a senior member of the Senior Executive Service, not lower than the equivalent of a 3-star general officer, or by exception a comparable military officer with extensive cyber experience;

''(B) exclusively occupy the Principal Cyber Advisor position and not assume any other position or responsibility in the relevant military department;

''(C) be independent of the relevant service's chief information officer; and

''(D) report directly to and advise the secretary of the relevant military department and advise the relevant service's senior uniformed officer.

''(3) NOTIFICATION.—Each of the secretaries of the military departments shall notify the Committees on Armed Services of the Senate and House of Representatives of his or her Principal Cyber Advisor appointment. In the case that the appointee is a military officer, the notification shall include a justification for the selection and an explanation of the appointee's ability to execute the responsibilities of the Principal Cyber Advisor.

''(b) RESPONSIBILITIES OF PRINCIPAL CYBER ADVISORS.—Each Principal Cyber Advisor under subsection (a) shall be responsible for advising both the secretary of the relevant military department and the senior uniformed military officer of the relevant military service and implementing the Department of Defense Cyber Strategy within the service by coordinating and overseeing the execution of the service's policies and programs relevant to the following:

''(1) The recruitment, resourcing, and training of military cyberspace operations forces, assessment of these forces against standardized readiness metrics, and maintenance of these forces at standardized readiness levels.

''(2) Acquisition of offensive, defensive, and Department of Defense Information Networks cyber capabilities for military cyberspace operations.

''(3) Cybersecurity management and operations.

''(4) Acquisition of cybersecurity tools and capabilities, including those used by cybersecurity service providers.

''(5) Evaluating, improving, and enforcing a culture of cybersecurity warfighting and accountability for cybersecurity and cyberspace operations.

''(6) Cybersecurity and related supply chain risk management of the industrial base.

''(7) Cybersecurity of Department of Defense information systems, information technology services, and weapon systems, including the incorporation of cybersecurity threat information as part of secure development processes, cybersecurity testing, and the mitigation of cybersecurity risks.

''(c) COORDINATION.—To ensure service compliance with the Department of Defense Cyber Strategy, each Principal Cyber Advisor under subsection (a) shall work in close coordination with the following:

''(1) Service chief information officers.

''(2) Service cyber component commanders.

''(3) Principal Cyber Advisor to the Secretary of Defense.

''(4) Department of Defense Chief Information Officer.

''(5) Defense Digital Service.

''(d) BUDGET CERTIFICATION AUTHORITY.—

''(1) IN GENERAL.—Each of the secretaries of the military departments shall require service components with responsibilities associated with cyberspace operations forces, offensive or defensive cyberspace operations and capabilities, and cyberspace issues relevant to the duties specified in subsection (b) to transmit the proposed budget for such responsibilities for a fiscal year and for the period covered by the future-years defense program submitted to Congress under section 221 of title 10, United States Code, for that fiscal year to the relevant service's Principal Cyber Advisor for review under subparagraph (B) before submitting the proposed budget to the department's comptroller.

''(2) REVIEW.—Each Principal Cyber Advisor under subsection (a)(1) shall review each proposed budget transmitted under paragraph (1) and submit to the secretary of the relevant military department a report containing the comments of the Principal Cyber Advisor with respect to all such proposed budgets, together with the certification of the Principal Cyber Advisor regarding whether each proposed budget is adequate.

''(3) REPORT.—Not later than March 31 of each year, each of the secretaries of the military departments shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report specifying each proposed budget for the subsequent fiscal year contained in the most-recent report submitted under paragraph (2) that the Principal Cyber Advisor did not certify to be adequate. The report of the secretary shall include a discussion of the actions that the secretary took or proposes to take, together with any additional comments that the Secretary considers appropriate regarding the adequacy or inadequacy of the proposed budgets.

''(e) PRINCIPAL CYBER ADVISORS' BRIEFING TO CONGRESS.—Not later than February 1, 2021, and biannually thereafter, each Principal Cyber Advisor under subsection (a) shall brief the Committees on Armed Services of the Senate and House of Representatives on that Advisor's activities and ability to perform the functions specified in subsection (b).

''(f) REVIEW OF CURRENT RESPONSIBILITIES.—

''(1) IN GENERAL.—Not later than January 1, 2021, each of the secretaries of the military departments shall review the relevant military department's current governance model for cybersecurity with respect to current authorities and responsibilities.

''(2) ELEMENTS.—Each review under paragraph (1) shall include the following:

''(A) An assessment of whether additional changes beyond the appointment of a Principal Cyber Advisor pursuant to subsection (a) are required.

''(B) Consideration of whether the current governance structure and assignment of authorities—

''(i) enable effective governance;

''(ii) enable effective Chief Information Officer and Chief Information Security Officer action;

''(iii) are adequately consolidated so that the authority and responsibility for cybersecurity risk management are clear and at an appropriate level of seniority;

''(iv) provide authority to a single individual to certify compliance of Department of Defense information systems and information technology services with all current cybersecurity standards; and

''(v) support efficient coordination across the military services, the Office of the Secretary of Defense, the Defense Information Systems Agency, and United States Cyber Command.

''(3) BRIEFING.—Not later than October 1, 2020, each of the secretaries of the military departments shall brief the Committees on Armed Services of the Senate and House of Representatives on the findings of

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