''(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.)

Editorial Notes

REFERENCES IN TEXT

Sections 1533 and 1534 of the National Defense Authorization Act for Fiscal Year 2023, referred to in subsec. (a)(1), are sections 1533 and 1534 of Pub. L. 117–263, also known as the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, which are set out as notes under section 167b of this title.

Statutory Notes and Related Subsidiaries

FIRST REPORT

Pub. L. 117–263, div. A, title XV, § 1502(b), Dec. 23, 2022, 136 Stat. 2880, provided that: ''The Commander of the United States Cyber Command shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] the first report under section 391a of title 10, United States Code, as added by subsection (a), as soon as practicable after the date of the submission of the defense budget materials for fiscal year 2024.''

§ 391b. Strategic cybersecurity program

(a) IN GENERAL.—(1) There is a program to be known as the ''Strategic Cybersecurity Program'' (in this section referred to as the ''Program'') to ensure the ability of the Department of Defense to conduct the most critical military missions of the Department.

(2) The Secretary of Defense shall designate a principal staff assistant from within the Office of the Secretary of Defense whose office shall serve as the office of primary responsibility for the Program, and provide policy, direction, and oversight regarding the execution of the responsibilities of the program manager selected pursuant to subsection (c)(1).

(b) MEMBERSHIP.—In addition to the office of primary responsibility for the Program under subsection (a)(2) and the program manager selected pursuant to subsection (c)(1), membership in the Program shall include the following:

(1) The Vice Chairman of the Joint Chiefs of Staff.

(2) The Commanders of the United States Cyber Command, United States European Command, United States Indo-Pacific Command, United States Northern Command, United States Strategic Command, United States Space Command, United States Transportation Command.

(3) The Under Secretary of Defense for Acquisition and Sustainment.

(4) The Under Secretary of Defense for Policy.

(5) The Chief Information Officer of the Department of Defense.

(6) The Chief Digital and Artificial Intelligence Officer of the Department of Defense.

(7) The chief information officers of the military departments.

(8) The Principal Cyber Advisor of the Department of Defense.

(9) The Principal Cyber Advisors of the military departments.

(10) Each senior official identified pursuant to subsection (i) of section 1647 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1118).

(11) Such other officials as may be determined necessary by the Secretary of Defense.

(c) PROGRAM OFFICE.—(1) There is in the Cybersecurity Directorate of the National Security Agency a program office to support the Program by identifying threats to, vulnerabilities in, and remediations for, the missions and mission elements specified in subsection (d)(1). Such program office shall be headed by a program manager selected by the Director of the National Security Agency.

(2) The Chief Information Officer of the Department of Defense, in exercising authority, direction, and control over the Cybersecurity Directorate of the National Security Agency, shall ensure that the program office under paragraph (1) is responsive to the requirements and direction of the program manager selected pursuant to such paragraph.

(3) The Secretary may augment the personnel assigned to the program office under paragraph (1) by assigning personnel as appropriate from among members of any covered armed force (including the reserve components thereof), civilian employees of the Department of Defense (including the Defense Intelligence Agency), and personnel of the research laboratories of the Department of Defense, who have particular expertise in the areas of responsibility referred to in subsection (d).

(d) DESIGNATION OF MISSION ELEMENTS OF PROGRAM.—(1) The Under Secretary of Defense for Policy, the Under Secretary of Defense for Acquisition and Sustainment, and the Vice Chairman of the Joint Chiefs of Staff shall identify and designate for inclusion in the Program all of the systems, critical infrastructure, kill chains, and processes, including systems and components in development, that comprise the following military missions of the Department of Defense:

(A) Nuclear deterrence and strike.

(B) Select long-range conventional strike missions germane to the warfighting plans of the United States European Command and the United States Indo-Pacific Command.

(C) Offensive cyber operations.

(D) Homeland missile defense.

(2) The Vice Chairman of the Joint Chiefs of Staff shall coordinate the identification and prioritization of the missions and mission components, and the development and approval of requirements relating to the cybersecurity of the missions and mission components, of the Program.

(e) ADDITIONAL RESPONSIBILITIES OF HEAD OF OFFICE OF PRIMARY RESPONSIBILITY.—In addition to providing policy, direction, and oversight as specified in subsection (a)(2), the head of the office of primary responsibility for the Program designated under such subsection shall be responsible—

(1) for overseeing and providing direction on any covered statutory requirement that is ongoing, recurrent (including on an annual basis), or unfulfilled, including by—

(A) reviewing any materials required to be submitted to Congress under the covered statutory requirement prior to such submission; and

(B) ensuring such submissions occur by the applicable deadline under the covered statutory requirement; and