tion, or withdrawal of nuclear weapons of the United States that are based in Europe made to ensure the safety, security, reliability, and credibility of such weapons.

(c) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means—

(1) the Committees on Armed Services of the House of Representatives and the Senate; and

(2) the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate.

(Added Pub. L. 112–239, div. A, title X, § 1037(b)(1), Jan. 2, 2013, 126 Stat. 1926; amended Pub. L. 117–81, div. A, title XVI, § 1635, Dec. 27, 2021, 135 Stat. 2091.)

Editorial Notes

AMENDMENTS

2021—Subsec. (b)(1). Pub. L. 117–81 substituted ''120 days'' for ''60 days''.

§ 497a. Notification required for reduction or consolidation of dual-capable aircraft based in Europe

(a) NOTIFICATION.—Not less than 90 days before the date on which the Secretary of Defense reduces or consolidates the dual-capable aircraft of the United States that are based in Europe, the Secretary shall submit to the congressional defense committees a notification of such planned reduction or consolidation, including the following:

(1) The reasons for such planned reduction or consolidation.

(2) Any effects of such planned reduction or consolidation on the extended deterrence mission of the United States.

(3) The manner in which the military requirements of the North Atlantic Treaty Organization (NATO) will continue to be met in light of such planned reduction or consolidation.

(4) A statement by the Secretary on the response of NATO to such planned reduction or consolidation.

(5) Whether there is any change in the force posture of the Russian Federation as a result of such planned reduction or consolidation, including with respect to the nonstrategic nuclear weapons of Russia that are within range of the member states of NATO.

(b) DUAL-CAPABLE AIRCRAFT DEFINED.—In this section, the term ''dual-capable aircraft'' means aircraft that can perform both conventional and nuclear missions.

(Added Pub. L. 113–66, div. A, title X, § 1051(b)(1), Dec. 26, 2013, 127 Stat. 858.)

§ 498. Unilateral change in nuclear weapons stockpile of the United States

(a) IN GENERAL.—Other than pursuant to a treaty to which the Senate has provided advice and consent pursuant to section 2 of article II of the Constitution of the United States, if the President has under consideration to unilaterally change the size of the total stockpile of nuclear weapons of the United States, or the total number of deployed nuclear weapons (as defined under the New START Treaty), by more than 20 percent, prior to doing so the President shall initiate a Nuclear Posture Review.

(b) TERMS OF REFERENCE.—Prior to the initiation of a Nuclear Posture Review under this section, the President shall determine the terms of reference for the Nuclear Posture Review, which the President shall provide to the congressional defense committees.

(c) NUCLEAR POSTURE REVIEW.—Upon completion of a Nuclear Posture Review under this section, the President shall submit the Nuclear Posture Review to the congressional defense committees prior to implementing any change described in subsection (a).

(d) CONSTRUCTION.—This section shall not apply to changes to the nuclear weapons stockpile resulting from obligations pursuant to a treaty to which the Senate has provided advice and consent pursuant to section 2 of article II of the Constitution.

(e) FORM.—A Nuclear Posture Review under this section shall be submitted in unclassified form, but may include a classified annex.

(f) NEW START TREATY DEFINED.—In this section, the term ''New START Treaty'' means the Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms, signed on April 8, 2010, and entered into force on February 5, 2011.

(Added Pub. L. 112–239, div. A, title X, § 1038(a), Jan. 2, 2013, 126 Stat. 1927; amended Pub. L. 113–66, div. A, title X, § 1091(a)(6), Dec. 26, 2013, 127 Stat. 875; Pub. L. 117–81, div. A, title XVI, § 1633, Dec. 27, 2021, 135 Stat. 2090.)

Editorial Notes

AMENDMENTS

2021—Subsec. (a). Pub. L. 117–81, § 1633(1), added subsec. (a) and struck out former subsec. (a). Prior to amendment, text read as follows: ''Other than pursuant to a treaty, if the President has under consideration to unilaterally change the size of the total stockpile of nuclear weapons of the United States by more than 25 percent, prior to doing so the President shall initiate a Nuclear Posture Review.''

Subsec. (c). Pub. L. 117–81, § 1633(2), substituted ''described in subsection (a)'' for ''in the nuclear weapons stockpile by more than 25 percent''.

Subsec. (d). Pub. L. 117–81, § 1633(3), substituted ''obligations pursuant to a treaty to which the Senate has provided advice and consent pursuant to section 2 of article II of the Constitution'' for ''treaty obligations''.

Subsec. (f). Pub. L. 117–81, § 1633(4), added subsec. (f).

2013—Pub. L. 113–66 inserted a period after the enumerator in section catchline.

§ 499. Annual assessment of cyber resiliency of nuclear command and control system

(a) IN GENERAL.—Not less frequently than annually, the Commander of the United States Strategic Command and the Commander of the United States Cyber Command (in this section referred to collectively as the ''Commanders'') shall jointly conduct an assessment of the cyber resiliency of the nuclear command and control system.

(b) ELEMENTS.—In conducting the assessment required by subsection (a), the Commanders shall—

(1) conduct an assessment of the sufficiency and resiliency of the nuclear command and control system to operate through a cyber attack from the Russian Federation, the People's Republic of China, or any other country or entity the Commanders identify as a potential threat; and

(2) develop recommendations for mitigating any concerns of the Commanders resulting from the assessment.

(c) REPORTS REQUIRED.—(1) For each assessment conducted under subsection (a), the Commanders shall jointly submit to the Chairman of the Joint Chiefs of Staff, for submission to the Council on Oversight of the National Leadership Command, Control, and Communications System established under section 171a of this title, a report on the assessment that includes the following:

(A) The recommendations developed under subsection (b)(2).

(B) A statement of the degree of confidence of each of the Commanders in the mission assurance of the nuclear deterrent against a top tier cyber threat.

(C) A detailed description of the approach used to conduct the assessment required by subsection (a) and the technical basis of conclusions reached in conducting that assessment.

(D) Any other comments of the Commanders.

(2) The Council shall submit to the Secretary of Defense each report required by paragraph (1) and any comments of the Council on each report.

(3) Not later than 90 days after the date of the submission of a report under paragraph (1), the Secretary of Defense shall submit to the congressional defense committees the report, any comments of the Council on the report under paragraph (2), and any comments of the Secretary on the report.

(d) QUARTERLY BRIEFINGS.—(1) Not less than once every quarter, the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff shall jointly provide to the Committees on Armed Services of the House of Representatives and the Senate—

(A) a briefing on any intrusion or anomaly in the nuclear command, control, and communications system that was identified during the previous quarter, including—

(i) an assessment of any known, suspected, or potential impacts of such intrusions and anomalies to the mission effectiveness of military capabilities as of the date of the briefing; and

(ii) with respect to cyber intrusions of contractor networks known or suspected to have resulted in the loss or compromise of design information regarding the nuclear command, control, and communications system; or

(B) if no such intrusion or anomaly occurred with respect to the quarter to be covered by that briefing, a notification of such lack of intrusions and anomalies.

(2) In this subsection:

(A) The term ''anomaly'' means a malicious, suspicious or abnormal cyber incident that potentially threatens the national security or interests of the United States, or that is likely to result in demonstrable harm to the national security of the United States.

(B) The term ''intrusion'' means an unauthorized and malicious cyber incident that compromises a nuclear command, control, and communications system by breaking the security of such a system or causing it to enter into an insecure state.

(e) TERMINATION.—The requirements of this section shall terminate on December 31, 2032.

(Added Pub. L. 115–91, div. A, title XVI, §1651(a), Dec. 12, 2017, 131 Stat. 1756; amended Pub. L. 117–81, div. A, title XV, §1534, Dec. 27, 2021, 135 Stat. 2054; Pub. L. 117–263, div. A, title XVI, §1636(a), (b), Dec. 23, 2022, 136 Stat. 2940.)

Editorial Notes

AMENDMENTS

2022—Subsec. (d). Pub. L. 117–263, §1636(a), amended subsec. (d) generally. Prior to amendment, text read as follows: ''Not less than once every quarter, the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff shall jointly provide to the Committees on Armed Services of the House of Representatives and the Senate a briefing on any known or suspected critical intelligence parameter breaches that were identified during the previous quarter, including an assessment of any known or suspected impacts of such breaches to the mission effectiveness of military capabilities as of the date of the briefing or thereafter.''

Subsec. (e). Pub. L. 117–263, §1636(b), substituted ''December 31, 2032'' for ''December 31, 2027''.

2021—Subsec. (c). Pub. L. 117–81, §1534(1), substituted ''Reports'' for ''Report'' in heading.

Subsec. (c)(1). Pub. L. 117–81, §1534(2), substituted ''For each assessment conducted under subsection (a), the Commanders'' for ''The Commanders'' and ''the assessment'' for ''the assessment required by subsection (a)'' in introductory provisions.

Subsec. (c)(2). Pub. L. 117–81, §1534(3), which directed substitution of ''each report'' for ''the report'', was executed by making the substitution in both places it appeared, to reflect the probable intent of Congress.

Subsec. (c)(3). Pub. L. 117–81, §1534(4), substituted ''Not later than 90 days after the date of the submission of a report under paragraph (1), the Secretary'' for ''The Secretary'' and struck out ''required by paragraph (1)'' before '', any comments''.

Statutory Notes and Related Subsidiaries

CYBERSECURITY ENHANCEMENTS FOR NUCLEAR COMMAND, CONTROL, AND COMMUNICATIONS NETWORK

Pub. L. 118–31, div. A, title XV, §1512, Dec. 22, 2023, 137 Stat. 542, provided that:

''(a) ESTABLISHMENT OF CROSS-FUNCTIONAL TEAM.—

''(1) ESTABLISHMENT.—Not later than 180 days after the date of the enactment of this Act [Dec. 22, 2023], and consistent with section 911(c) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 10 U.S.C. 111 note), the Secretary of Defense shall establish a cross-functional team to develop and direct the implementation of a threat-driven cyber defense construct for the systems and networks that support the nuclear command, control, and communications (commonly referred to as 'NC3') mission (in this section referred to as the 'cross-functional team').

''(2) COMPOSITION OF CROSS-FUNCTIONAL TEAM.—

''(A) IN GENERAL.—The cross functional team shall be composed of senior officers selected from among each of the military departments, the Defense Information Systems Agency, the National Security Agency, the United States Cyber Command, the United States Strategic Command, and any other organization or element of the Department of Defense determined appropriate by the Secretary.

''(B) LEADERSHIP.—The Secretary shall designate a senior officer from those selected under subparagraph (A) to serve as the leader of the cross-functional team.

''(C) STAFF.—The Secretary shall ensure the heads of the organizations and elements specified in subparagraph (A) detail staff to support the cross-functional team in carrying out the duties under paragraph (3).

''(3) DUTIES.—The duties of the cross-functional team shall be to enhance the cyber defense of the systems and networks that support the nuclear command, control, and communications mission.

''(b) REQUIRED CONSTRUCT, PLAN OF ACTION, AND MILESTONES.—Not later than one year after the date of the enactment of this Act, the leader of the cross-functional team designated pursuant to subsection (a)(2)(B) shall develop a threat-driven cyber defense construct, and associated plans and milestones, to enhance the security of the systems and networks that support the nuclear command, control, and communications mission. Such construct shall be based on—

''(1) the application of the principles of the approach to cybersecurity commonly referred to as 'zero trust architecture';

''(2) an analysis of appropriately comprehensive endpoint and network telemetry data; and

''(3) control capabilities enabling rapid investigation and remediation of indicators of compromise and threats to mission execution.

''(c) ANNUAL BRIEFINGS.—During the 60-day period beginning on the date that is 30 days before the date on which the President submits to Congress the budget of the President pursuant to section 1105(a) of title 31, United States Code, for each of fiscal years 2025 through 2028, the Secretary shall provide to the appropriate congressional committees a briefing on the implementation of this section.

''(d) TERMINATION.—

''(1) IN GENERAL.—Except as provided in paragraph (2), the cross-functional team under this section shall terminate on October 31, 2028.

''(2) EXTENSION AUTHORITY.—The Secretary of Defense may extend the date of termination under paragraph (1) as the Secretary determines appropriate.

''(e) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term 'appropriate congressional committees' means—

''(1) the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives]; and

''(2) the Permanent Select Committee on Intelligence of the House of Representatives.''

ENSURING CYBER RESILIENCY OF NUCLEAR COMMAND AND CONTROL SYSTEM

Pub. L. 116–283, div. A, title XVII, §1747, Jan. 1, 2021, 134 Stat. 4140, provided that:

''(a) PLAN FOR IMPLEMENTATION OF FINDINGS AND RECOMMENDATIONS FROM FIRST ANNUAL ASSESSMENT OF CYBER RESILIENCY OF NUCLEAR COMMAND AND CONTROL SYSTEM.—Not later than October 1, 2021, the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a comprehensive plan, including a schedule and resourcing plan, for the implementation of the findings and recommendations included in the first report submitted under section 499(c)(3) of title 10, United States Code.

''(b) CONCEPT OF OPERATIONS AND OVERSIGHT MECHANISM FOR CYBER DEFENSE OF NUCLEAR COMMAND AND CONTROL SYSTEM.—Not later than October 1, 2021, the Secretary shall develop and establish—

''(1) a concept of operations for defending the nuclear command and control system against cyber attacks, including specification of the—

''(A) roles and responsibilities of relevant entities within the Office of the Secretary, the military services, combatant commands, the Defense Agencies, and the Department of Defense Field Activities; and

''(B) cybersecurity capabilities to be acquired and employed and operational tactics, techniques, and procedures, including cyber protection team and sensor deployment strategies, to be used to monitor, defend, and mitigate vulnerabilities in nuclear command and control systems; and

''(2) an oversight mechanism or governance model for overseeing the implementation of the concept of operations developed and established under paragraph (1), related development, systems engineering, and acquisition activities and programs, and the plan required by subsection (a), including specification of the—

''(A) roles and responsibilities of relevant entities within the Office of the Secretary, the military services, combatant commands, the Defense Agencies, and the Department of Defense Field Activities in overseeing the defense of the nuclear command and control system against cyber attacks;

''(B) responsibilities and authorities of the Strategic Cybersecurity Program in overseeing and, as appropriate, executing—

''(i) vulnerability assessments; and

''(ii) development, systems engineering, and acquisition activities; and

''(C) processes for coordination of activities, policies, and programs relating to the cybersecurity and defense of the nuclear command and control system.''

§ 499a. Collection, storage, and sharing of data relating to nuclear security enterprise and nuclear forces

(a) IN GENERAL.—The Secretary of Defense, acting through the Director of Cost Assessment and Program Evaluation, and the Administrator for Nuclear Security, acting through the Director for Cost Estimating and Program Evaluation, shall collect and store cost, programmatic, and technical data relating to programs and projects of the nuclear security enterprise and nuclear forces.

(b) SHARING OF DATA.—If the Director of Cost Assessment and Program Evaluation or the Director for Cost Estimating and Program Evaluation requests data relating to programs or projects from any element of the Department of Defense or from any element of the nuclear security enterprise of the National Nuclear Security Administration, that element shall provide that data in a timely manner.

(c) STORAGE OF DATA.—(1) Data collected by the Director of Cost Assessment and Program Evaluation and the Director for Cost Estimating and Program Evaluation under this section shall be—

(A) stored in the data storage system of the Defense Cost and Resource Center, or successor center, or in a data storage system of the National Nuclear Security Administration that is comparable to the data storage system of the Defense Cost and Resource Center; and

(B) made accessible to other Federal agencies as such Directors consider appropriate.

(2) The Secretary and the Administrator shall ensure that the Director of Cost Assessment and