to subpar. (D) by Pub. L. 116–283, see 2021 Amendment note above.

Pub. L. 116–92, § 902(8)(B), added subpar. (C). Former subpar. (C) redesignated (D).

Subsec. (b)(2)(D) to (F). Pub. L. 116–92, § 902(8)(C), redesignated subpars. (C) to (E) as (D) to (F), respectively.

2015—Pub. L. 114–92, § 1641(a)(1), substituted ''Reporting on penetrations of networks and information systems of certain contractors'' for ''Reports to Department of Defense on penetrations of networks and information systems of certain contractors'' in section catchline.

Pub. L. 114–92, § 1641(a), transferred section 941 of Pub. L. 112–239 to this chapter and renumbered it as this section. See Codification note above.

Subsec. (c)(3). Pub. L. 114–92, § 1641(a)(2), added par. (3) and struck out former par. (3). Prior to amendment, text read as follows: ''The procedures established pursuant to subsection (a) shall prohibit the dissemination outside the Department of Defense of information obtained or derived through such procedures that is not created by or for the Department except with the approval of the contractor providing such information.''

Subsec. (d). Pub. L. 114–92, § 1641(a)(3), added subsec. (d) and struck out former subsec. (d). Prior to amendment, text read as follows:

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act—

''(A) the Secretary of Defense shall establish the procedures required under subsection (a); and

''(B) the senior official designated under subsection (b)(1) shall establish the criteria required under such subsection.

''(2) APPLICABILITY DATE.—The requirements of this section shall apply on the date on which the Secretary of Defense establishes the procedures required under this section.''

§ 394. Authorities concerning military cyber operations

(a) IN GENERAL.—The Secretary of Defense shall develop, prepare, and coordinate; make ready all armed forces for purposes of; and, when appropriately authorized to do so, conduct, military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power.

(b) AFFIRMATION OF AUTHORITY.—Congress affirms that the activities or operations referred to in subsection (a), when appropriately authorized, include the conduct of military activities or operations in cyberspace short of hostilities (as such term is used in the War Powers Resolution (Public Law 93–148; 50 U.S.C. 1541 et seq.)) or in areas in which hostilities are not occurring, including for the purpose of preparation of the environment, information operations, force protection, and deterrence of hostilities, or counterterrorism operations involving the Armed Forces of the United States.

(c) CLANDESTINE ACTIVITIES OR OPERATIONS.—A clandestine military activity or operation in cyberspace shall be considered a traditional military activity for the purposes of section 503(e)(2) of the National Security Act of 1947 (50 U.S.C. 3093(e)(2)).

(d) CONGRESSIONAL OVERSIGHT.—The Secretary shall brief the congressional defense committees about any military activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, occurring during the previous quarter during the quarterly briefing required by section 484 of this title.

(e) RULE OF CONSTRUCTION.—Nothing in this section may be construed to limit the authority of the Secretary to conduct military activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to authorize specific military activities or operations, or to alter or otherwise affect the War Powers Resolution (50 U.S.C. 1541 et seq.), the Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note), or reporting of sensitive military cyber activities or operations required by section 395 of this title.

(f) DEFINITIONS.—In this section:

(1) The term ''clandestine military activity or operation in cyberspace'' means a military activity or military operation carried out in cyberspace, or associated preparatory actions, authorized by the President or the Secretary that—

(A) is marked by, held in, or conducted with secrecy, where the intent is that the activity or operation will not be apparent or acknowledged publicly; and

(B) is to be carried out—

(i) as part of a military operation plan approved by the President or the Secretary in anticipation of hostilities or as directed by the President or the Secretary;

(ii) to deter, safeguard, or defend against attacks or malicious cyber activities against the United States or Department of Defense information, networks, systems, installations, facilities, or other assets; or

(iii) in support of information related capabilities.

(2) The term ''foreign power'' has the meaning given such term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(3) The term ''United States person'' has the meaning given such term in such section.

(Added Pub. L. 114–92, div. A, title XVI, § 1642(a), Nov. 25, 2015, 129 Stat. 1116, § 130g; renumbered § 394 and amended Pub. L. 115–232, div. A, title XVI, §§ 1631(a), 1632, Aug. 13, 2018, 132 Stat. 2123.)

Editorial Notes

REFERENCES IN TEXT

The War Powers Resolution, referred to in subsecs. (b) and (e), is Pub. L. 93–148, Nov. 7, 1973, 87 Stat. 555, which is classified generally to chapter 33 (§ 1541 et seq.) of Title 50, War and National Defense. For complete classification of this Resolution to the Code, see Short Title note set out under section 1541 of Title 50 and Tables.

The Authorization for Use of Military Force, referred to in subsec. (e), is Pub. L. 107–40, Sept. 18, 2001, 115 Stat. 224, which is set out as a note under section 1541 of Title 50, War and National Defense.

AMENDMENTS

2018—Pub. L. 115–232, § 1632, designated existing provisions as subsec. (a), inserted heading, substituted ''conduct, military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response'' for ''conduct, a mili-

tary cyber operation in response'', struck out ''(as such terms are defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801))'' after ''foreign power'', and added subsecs. (b) to (f).

Pub. L. 115–232, §1631(a), renumbered section 130g of this title as this section.

Statutory Notes and Related Subsidiaries

SUPPORT FOR CYBER THREAT TABLETOP EXERCISE PROGRAM WITH THE DEFENSE INDUSTRIAL BASE

Pub. L. 118–159, div. A, title XV, §1504, Dec. 23, 2024, 138 Stat. 2133, provided that:

''(a) DEVELOPMENT OF CYBER THREAT TABLETOP EXERCISE PROGRAM.—

''(1) IN GENERAL.— Not later than one year after the date of the enactment of this Act [Dec. 23, 2024], the Secretary of Defense, acting through the Assistant Secretary of Defense for Cyber Policy, shall establish a program (to be known as the 'Cyber Threat Tabletop Exercise Program') to prepare the Department of Defense and the defense industrial base for cyber attacks preceding or during times of conflict or wars through the use of tabletop exercises.

''(2) PARTICIPATION.—

''(A) IN GENERAL.—In carrying out the program, the Secretary of Defense, acting through the Assistant Secretary of Defense for Cyber Policy, shall consult and coordinate with the following:

''(i) The Chief Information Officer of the Department of Defense.

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

''(iii) The Commander of the United States Cyber Command.

''(iv) The Commander of the United States Northern Command.

''(v) The Commander of the Army Interagency Training and Education Center.

''(vi) The Director of the Defense Cyber Crime Center.

''(vii) Such other individuals and entities as the Assistant Secretary of Defense for Cyber Policy determines appropriate.

''(B) SOLICITATION.—The Assistant Secretary of Defense for Cyber Policy may solicit such individuals and entities in the Department of Defense and the defense industrial base as the Assistant Secretary determines appropriate to participate in the program.

''(3) CYBER THREAT TABLETOP EXERCISE PROGRAM.——

''(A) IN GENERAL.—The program shall consist of the following:

''(i) A series of tabletop exercises that simulate cyber attack scenarios affecting the defense industrial base, which the Assistant Secretary of Defense for Cyber Policy shall carry out on a biannual basis beginning not later than one year after the date of the enactment of this Act until December 30, 2030, and in which the Department of Defense and entities in the defense industrial base shall participate.

''(ii) A series of tabletop exercises for use by individual entities or collections of entities in the defense industrial base that simulate cyber attack scenarios affecting the defense industrial base and which are designed to test and improve the responses and plans of such entities to such scenarios.

''(B) TABLETOP EXERCISE DEVELOPMENT.—

''(i) IN GENERAL.—The Assistant Secretary of Defense for Cyber Policy shall develop and update the tabletop exercises described in subparagraph (A).

''(ii) REALISTIC ATTACKS.—The Assistant Secretary of Defense for Cyber Policy shall ensure that the cyber attacks simulated by the tabletop exercises described in subparagraph (A) are based on the cyber attack capabilities and activities of current and potential adversaries of the United States.

''(4) PROCEDURES FOR IDENTIFICATION OF VULNERABILITIES AND LESSONS LEARNED.—Not later than one year after the date of the enactment of this Act, the Assistant Secretary of Defense for Cyber Policy shall establish procedures to—

''(A) identify vulnerabilities in the cybersecurity of the Department of Defense and the defense industrial base pursuant to the tabletop exercises carried out under the program; and

''(B) identify other lessons learned that can improve national security or the quality of such tabletop exercises.

''(b) ANNUAL REPORT.—Not later than September 30, 2025, and annually thereafter until the [sic] October 1, 2029, the Secretary of Defense, acting through the Assistant Secretary of Defense for Cyber Policy, shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report describing the activities of the Department of Defense pursuant to this section during the preceding year.

''(c) PROGRAM DEFINED.—In this section, the term 'program' means the program established under subsection (a).''

AUTHORITY FOR COUNTERING ILLEGAL TRAFFICKING BY MEXICAN TRANSNATIONAL CRIMINAL ORGANIZATIONS IN CYBERSPACE

Pub. L. 118–31, div. A, title XV, §1505, Dec. 22, 2023, 137 Stat. 539, provided that:

''(a) AUTHORITY.—In accordance with sections 124 and 394 of title 10, United States Code, the Secretary of Defense, in support of and in coordination with the heads of other relevant Federal departments and agencies and in consultation with the Government of Mexico as appropriate, may conduct detection, monitoring, and other operations in cyberspace to counter Mexican transnational criminal organizations that are engaged in any of the following activities that cross the southern border of the United States:

''(1) Smuggling of illegal drugs, controlled substances, or precursors thereof.

''(2) Human trafficking.

''(3) Weapons trafficking.

''(4) Other illegal activities.

''(b) CERTAIN ENTITIES.—The authority under paragraph (1) [probably should be ''subsection (a)''] may be used to counter Mexican transnational criminal organizations, including entities cited in the most recent National Drug Threat Assessment published by the United States Drug Enforcement Administration, that are engaged in any of the activities described in such paragraph.''

MANAGEMENT OF DATA ASSETS BY CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER

Pub. L. 118–31, div. A, title XV, §1523, Dec. 22, 2023, 137 Stat. 553, provided that:

''(a) IN GENERAL.—The Secretary of Defense, subject to existing authorities and limitations and acting through the Chief Digital and Artificial Intelligence Officer of the Department of Defense, shall provide the digital infrastructure and procurement vehicles necessary to manage data assets and data analytics capabilities at scale to enable an understanding of foreign key terrain and relational frameworks in cyberspace to support the planning of cyber operations, the generation of indications and warnings regarding military operations and capabilities, and the calibration of actions and reactions in strategic competition.

''(b) RESPONSIBILITIES OF CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER.—The Chief Digital and Artificial Intelligence Officer shall—

''(1) develop a baseline of data assets exclusive to foreign key terrain and relational frameworks in cyberspace maintained by the intelligence agencies of

the Department of Defense, the military departments, the combatant commands, and any other components of the Department of Defense;

''(2) develop and oversee the implementation of plans to enhance such data assets that the Chief Digital and Artificial Intelligence Officer determines are essential to support the purposes set forth in subsection (a); and

''(3) ensure that such activities and plans are undertaken in cooperation and in coordination with the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, to ensure that any data collection, procurement, acquisition, use, or retention measure conducted pursuant to this section is in compliance with applicable laws and regulations, including standards pertaining to data related to United States persons or any persons in the United States.

''(c) OTHER MATTERS.—The Chief Digital and Artificial Intelligence Officer shall—

''(1) designate or establish one or more Department of Defense executive agents for enhancing data assets and the acquisition of data analytic tools for users;

''(2) ensure that data assets referred to in subsection (b) that are in the possession of a component of the Department of Defense are accessible for the purposes described in subsection (a); and

''(3) ensure that advanced analytics, including artificial intelligence technology, are developed and applied to the analysis of the data assets referred to in subsection (b) in support of the purposes described in subsection (a).

''(d) SEMIANNUAL BRIEFINGS.—Not later than 120 days after the date of the enactment of this Act [Dec. 22, 2023], and not less frequently than semiannually thereafter, the Chief Digital and Artificial Intelligence Officer shall provide to the appropriate congressional committees a briefing on the implementation of this section.

''(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to authorize the Department of Defense to collect, procure, or otherwise acquire data, including commercially available data, in any manner that is not authorized by law, or to make use of data assets in any manner, or for any purpose, that is not otherwise authorized by law.

''(f) 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];

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

''(3) the Select Committee on Intelligence of the Senate.''

PROTECTION OF CRITICAL INFRASTRUCTURE

Pub. L. 117–263, div. A, title XV, § 1511, Dec. 23, 2022, 136 Stat. 2892, provided that:

''(a) IN GENERAL.—In the event that the President determines that there is an active, systematic, and ongoing campaign of attacks in cyberspace by a foreign power against the Government or the critical infrastructure of the United States, the President may authorize the Secretary of Defense, acting through the Commander of the United States Cyber Command, to conduct military cyber activities or operations pursuant to section 394 of title 10, United States Code, in foreign cyberspace to deter, safeguard, or defend against such attacks.

''(b) AFFIRMATION OF SCOPE OF CYBER ACTIVITIES OR OPERATIONS.—Congress affirms that the cyber activities or operations referred to in subsection (a), when appropriately authorized, shall be conducted consistent with section 394 of title 10, United States Code.

''(c) DEFINITION OF CRITICAL INFRASTRUCTURE.—In this section, the term 'critical infrastructure' has the meaning given that term in subsection (e) [of section 1016] of the Critical Infrastructure[s] Protection Act of 2001 (42 U.S.C. 5195c(e)).''

OPERATIONAL TECHNOLOGY AND MISSION-RELEVANT TERRAIN IN CYBERSPACE

Pub. L. 117–81, div. A, title XV, § 1505, Dec. 27, 2021, 135 Stat. 2023, as amended by Pub. L. 118–31, div. A, title XV, § 1502(a)(2)(E), Dec. 22, 2023, 137 Stat. 538, provided that:

''(a) MISSION-RELEVANT TERRAIN.—Not later than January 1, 2025, the Secretary of Defense shall complete mapping of mission-relevant terrain in cyberspace for Defense Critical Assets and Task Critical Assets at sufficient granularity to enable mission thread analysis and situational awareness, including required—

''(1) decomposition of missions reliant on such Assets;

''(2) identification of access vectors;

''(3) internal and external dependencies;

''(4) topology of networks and network segments;

''(5) cybersecurity defenses across information and operational technology on such Assets; and

''(6) identification of associated or reliant weapon systems.

''(b) COMBATANT COMMAND RESPONSIBILITIES.—Not later than January 1, 2024, the Commanders of 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, and other relevant Commands, in coordination with the Commander of United States Cyber Command, in order to enable effective mission thread analysis, cyber situational awareness, and effective cyber defense of Defense Critical Assets and Task Critical Assets under their control or in their areas of responsibility, shall develop, institute, and make necessary modifications to—

''(1) internal combatant command processes, responsibilities, and functions;

''(2) coordination with service components under their operational control, United States Cyber Command, Joint Forces Headquarters-Department of Defense Information Network, and the service cyber components;

''(3) combatant command headquarters' situational awareness posture to ensure an appropriate level of cyber situational awareness of the forces, facilities, installations, bases, critical infrastructure, and weapon systems under their control or in their areas of responsibility, including, in particular, Defense Critical Assets and Task Critical Assets; and

''(4) documentation of their mission-relevant terrain in cyberspace.

''(c) DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER RESPONSIBILITIES.—

''(1) IN GENERAL.—Not later than November 1, 2023, the Chief Information Officer of the Department of Defense shall establish or make necessary changes to policy, control systems standards, risk management framework and authority to operate policies, and cybersecurity reference architectures to provide baseline cybersecurity requirements for operational technology in forces, facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network.

''(2) IMPLEMENTATION OF POLICIES.—The Chief Information Officer of the Department of Defense shall leverage acquisition guidance, concerted assessment of the Department's operational technology enterprise, and coordination with the military department principal cyber advisors and chief information officers to drive necessary change and implementation of relevant policy across the Department's forces, facilities, installations, bases, critical infrastructure, and weapon systems.

''(3) ADDITIONAL RESPONSIBILITIES.—The Chief Information Officer of the Department of Defense shall ensure that policies, control systems standards, and cybersecurity reference architectures—

''(A) are implementable by components of the Department;

''(B) limit adversaries' ability to reach or manipulate control systems through cyberspace;

''(C) appropriately balance non-connectivity and monitoring requirements;

''(D) include data collection and flow requirements;

''(E) interoperate with and are informed by the operational community's workflows for defense of information and operational technology in the forces, facilities, installations, bases, critical infrastructure, and weapon systems across the Department;

''(F) integrate and interoperate with Department mission assurance construct; and

''(G) are implemented with respect to Defense Critical Assets and Task Critical Assets.

''(d) UNITED STATES CYBER COMMAND OPERATIONAL RESPONSIBILITIES.—Not later than January 1, 2025, the Commander of United States Cyber Command shall make necessary modifications to the mission, scope, and posture of Joint Forces Headquarters-Department of Defense Information Network to ensure that Joint Forces Headquarters—

''(1) has appropriate visibility of operational technology in the forces, facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network, including, in particular, Defense Critical Assets and Task Critical Assets;

''(2) can effectively command and control forces to defend such operational technology; and

''(3) has established processes for—

''(A) incident and compliance reporting;

''(B) ensuring compliance with Department of Defense cybersecurity policy; and

''(C) ensuring that cyber vulnerabilities, attack vectors, and security violations, including, in particular, those specific to Defense Critical Assets and Task Critical Assets, are appropriately managed.

''(e) UNITED STATES CYBER COMMAND FUNCTIONAL RESPONSIBILITIES.—Not later than January 1, 2025, the Commander of United States Cyber Command shall—

''(1) ensure in its role of Joint Forces Trainer for the Cyberspace Operations Forces that operational technology cyber defense is appropriately incorporated into training for the Cyberspace Operations Forces;

''(2) delineate the specific force composition requirements within the Cyberspace Operations Forces for specialized cyber defense of operational technology, including the number, size, scale, and responsibilities of defined Cyber Operations Forces elements;

''(3) develop and maintain, or support the development and maintenance of, a joint training curriculum for operational technology-focused Cyberspace Operations Forces;

''(4) support the Chief Information Officer of the Department of Defense as the Department's senior official for the cybersecurity of operational technology under this section;

''(5) develop and institutionalize, or support the development and institutionalization of, tradecraft for defense of operational technology across local defenders, cybersecurity service providers, cyber protection teams, and service-controlled forces;

''(6) develop and institutionalize integrated concepts of operation, operational workflows, and cybersecurity architectures for defense of information and operational technology in the forces, facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network, including, in particular, Defense Critical Assets and Task Critical Assets, including—

''(A) deliberate and strategic sensoring of such Network and Assets;

''(B) instituting policies governing connections across and between such Network and Assets;

''(C) modelling of normal behavior across and between such Network and Assets;

''(D) engineering data flows across and between such Network and Assets;

''(E) developing local defenders, cybersecurity service providers, cyber protection teams, and service-controlled forces' operational workflows and tactics, techniques, and procedures optimized for the designs, data flows, and policies of such Network and Assets;

''(F) instituting of model defensive cyber operations and Department of Defense Information Network operations tradecraft; and

''(G) integrating of such operations to ensure interoperability across echelons; and

''(7) advance the integration of the Department of Defense's mission assurance, cybersecurity compliance, cybersecurity operations, risk management framework, and authority to operate programs and policies.

''(f) SERVICE RESPONSIBILITIES.—Not later than January 1, 2025, the Secretaries of the military departments, through the service principal cyber advisors, chief information officers, the service cyber components, and relevant service commands, shall make necessary investments in operational technology in the forces, facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network and the service-controlled forces responsible for defense of such operational technology to—

''(1) ensure that relevant local network and cybersecurity forces are responsible for defending operational technology across the forces, facilities, installations, bases, critical infrastructure, and weapon systems, including, in particular, Defense Critical Assets and Task Critical Assets;

''(2) ensure that relevant local operational technology-focused system operators, network and cybersecurity forces, mission defense teams and other service-retained forces, and cyber protection teams are appropriately trained, including through common training and use of cyber ranges, as appropriate, to execute the specific requirements of cybersecurity operations in operational technology;

''(3) ensure that all Defense Critical Assets and Task Critical Assets are monitored and defended by Cybersecurity Service Providers;

''(4) ensure that operational technology is appropriately sensored and appropriate cybersecurity defenses, including technologies associated with the More Situational Awareness for Industrial Control Systems Joint Capability Technology Demonstration, are employed to enable defense of Defense Critical Assets and Task Critical Assets;

''(5) implement Department of Defense Chief Information Officer policy germane to operational technology, including, in particular, with respect to Defense Critical Assets and Task Critical Assets;

''(6) plan for, designate, and train dedicated forces to be utilized in operational technology-centric roles across the military services and United States Cyber Command; and

''(7) ensure that operational technology, as appropriate, is not easily accessible via the internet and that cybersecurity investments accord with mission risk to and relevant access vectors for Defense Critical Assets and Task Critical Assets.

''(g) OFFICE OF THE SECRETARY OF DEFENSE RESPONSIBILITIES.—Not later than January 1, 2023, the Secretary of Defense shall—

''(1) assess and finalize Office of the Secretary of Defense components' roles and responsibilities for the cybersecurity of operational technology in the forces, facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network;

''(2) assess the need to establish centralized or dedicated funding for remediation of cybersecurity gaps in operational technology across the Department of Defense Information Network;

''(3) make relevant modifications to the Department of Defense's mission assurance construct, Mis-

sion Assurance Coordination Board, and other relevant bodies to drive—

''(A) prioritization of kinetic and non-kinetic threats to the Department's missions and minimization of mission risk in the Department's war plans;

''(B) prioritization of relevant mitigations and investments to harden and assure the Department's missions and minimize mission risk in the Department's war plans; and

''(C) completion of mission relevant terrain mapping of Defense Critical Assets and Task Critical Assets and population of associated assessment and mitigation data in authorized repositories;

''(4) make relevant modifications to the Strategic Cybersecurity Program; and

''(5) drive and provide oversight of the implementation of this section.

''(h) IMPLEMENTATION.—

''(1) IN GENERAL.—In implementing this section, the Secretary of Defense shall prioritize the cybersecurity and cyber defense of Defense Critical Assets and Task Critical Assets and shape cyber investments, policy, operations, and deployments to ensure cybersecurity and cyber defense.

''(2) APPLICATION.—This section shall apply to assets owned and operated by the Department of Defense, as well as to applicable non-Department assets essential to the projection, support, and sustainment of military forces and operations worldwide.

''(i) DEFINITION.—In this section:

''(1) MISSION-RELEVANT TERRAIN IN CYBERSPACE.—'mission-relevant [sic] terrain in cyberspace' has the meaning given such term as specified in Joint Publication 6-0.

''(2) OPERATIONAL TECHNOLOGY.—The term 'operational technology' means control systems or controllers, communication architectures, and user interfaces that monitor or control infrastructure and equipment operating in various environments, such as weapon systems, utility or energy production and distribution, or medical, logistics, nuclear, biological, chemical, or manufacturing facilities.''

FRAMEWORK FOR CYBER HUNT FORWARD OPERATIONS

Pub. L. 116–283, div. A, title XVII, §1720, Jan. 1, 2021, 134 Stat. 4107, provided that:

''(a) FRAMEWORK REQUIRED.—Not later than April 1, 2021, the Secretary of Defense shall develop a standard, comprehensive framework to enhance the consistency, execution, and effectiveness of cyber hunt forward operations.

''(b) ELEMENTS.—The framework developed pursuant to subsection (a) shall include the following:

''(1) Identification of the selection criteria for proposed cyber hunt forward operations, including specification of necessary thresholds for the justification of operations and thresholds for partner cooperation.

''(2) The roles and responsibilities of the following organizations in the support of the planning and execution of cyber hunt forward operations:

''(A) United States Cyber Command.

''(B) Service cyber components.

''(C) The Office of the Under Secretary of Defense for Policy.

''(D) Geographic combatant commands.

''(E) Cyber Operations-Integrated Planning Elements and Joint Cyber Centers.

''(F) Embassies and consulates of the United States.

''(3) Pre-deployment planning guidelines to maximize the operational success of each unique operation, including guidance that takes into account the highly variable nature of the following aspects at the tactical level:

''(A) Team composition, including necessary skillsets [sic], recommended training, and guidelines on team size and structure.

''(B) Relevant factors to determine mission duration in a country of interest.

''(C) Agreements with partner countries required pre-deployment.

''(D) Criteria for potential follow-on operations.

''(E) Equipment and infrastructure required to support the missions.

''(4) Metrics to measure the effectiveness of each operation, including means to evaluate the value of discovered malware and infrastructure, the effect on the adversary, and the potential for future engagements with the partner country.

''(5) Roles and responsibilities for United States Cyber Command and the National Security Agency in the analysis of relevant mission data.

''(6) A detailed description of counterintelligence support for cyber hunt forward operations.

''(7) A standardized force presentation model across service components and combatant commands.

''(8) Review of active and reserve component personnel policies to account for deployment and redeployment operations, including the following:

''(A) Global Force Management.

''(B) Contingency, Exercise, and Deployment orders to be considered for and applied towards deployment credit and benefits.

''(9) Such other matters as the Secretary determines relevant.

''(c) BRIEFING.—

''(1) IN GENERAL.—Not later than May 1, 2021, the Secretary of Defense shall provide to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives a briefing on the framework developed pursuant to subsection (a).

''(2) CONTENTS.—The briefing required by paragraph (1) shall include the following:

''(A) An overview of the framework developed pursuant to subsection (a).

''(B) An explanation of the tradeoffs associated with the use of Department of Defense resources for cyber hunt forward missions in the context of competing priorities.

''(C) Such recommendations as the Secretary may have for legislative action to improve the effectiveness of cyber hunt forward missions.''

TAILORED CYBERSPACE OPERATIONS ORGANIZATIONS

Pub. L. 116–283, div. A, title XVII, §1723, Jan. 1, 2021, 134 Stat. 4110, as amended by Pub. L. 117–263, div. A, title XV, §1504, Dec. 23, 2022, 136 Stat. 2880, provided that:

''(a) STUDY.—

''(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act [Jan. 1, 2021], the Secretary of the Navy and the Chief of Naval Operations, in consultation with the Commander of 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] a study of the Navy Cyber Warfare Development Group (NCWDG).

''(2) ELEMENTS.—The study required under paragraph (1) shall include the following:

''(A) An examination of NCWDG's structure, manning, authorities, funding, and operations.

''(B) A review of organizational relationships—

''(i) within the Navy; and

''(ii) to other Department of Defense organizations, as well as non-Department of Defense organizations.

''(C) Recommendations for how the NCWDG can be strengthened and improved, without growth in size.

''(D) Such other information as determined necessary or appropriate by the Secretary of the Navy.

''(3) RELEASE.—

''(A) TO CONGRESS.—Not later than 7 days after completion of the study required under paragraph (1), the Secretary of the Navy shall brief the congressional defense committees on the findings of the study.

''(B) TO SERVICE SERVICES.— The Secretary of the Navy shall transmit to the secretaries of the military services and the Assistant Secretary of Defense for Special Operations and Irregular Warfare the study required under paragraph (1).

''(b) DESIGNATION.—Notwithstanding any other provision of law, the Secretary of the Navy shall designate the NCWDG as a screened command.

''(c) AUTHORITY TO REPLICATE.—After review of the study required under subsection (a) and consulting the Commander of United States Cyber Command in accordance with procedures established by the Secretary of Defense, the secretaries of the military services may establish tailored cyberspace operations organizations of comparable size to NCWDG within the military service, respectively, of each such secretary. Such counterpart organizations shall have the same authorities as the NCWDG. On behalf of United States Special Operations Command, the Assistant Secretary of Defense for Special Operations and Irregular Warfare may authorize a tailored cyberspace operations organization within United States Special Operations Command of similar size and equivalent authorities as NCWDG.

''(d) BRIEFING TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act, the secretaries of the military services and the Assistant Secretary of Defense for Special Operations and Irregular Warfare shall brief the congressional defense committees on—

''(1) the utilization of the authority provided pursuant to subsection (c); and

''(2) if appropriate based on such utilization, details on how the military service, respectively, of each such secretary intends to establish tailored cyberspace operations organizations.

''(e) IMPLEMENTATION.—Not later than May 1, 2023, the Commanding Officer of Navy Cyber Warfare Development Group shall submit to the congressional defense committees an independent review of the study under subsection (a). The review shall include, at a minimum, evaluations of—

''(1) the value of the study to the Navy Cyber Warfare Development Group and to the Navy;

''(2) any recommendations not considered or included as part of the study;

''(3) the implementation of subsection (b); and

''(4) other matters as determined by the Commanding Officer.

''(f) UPDATE TO CONGRESS.—Not later than July 1, 2023, the Secretaries of the military departments and the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict shall provide to the congressional defense committees a briefing on activities taken during the period following the date of the briefing provided under subsection (d), including an examination of establishing Tailored Cyberspace Operations Organizations and use of the authority provided pursuant to subsection (c).

''(g) AIR FORCE ACTIONS.—Not later than July 1, 2023, the Secretary of the Air Force shall submit to the congressional defense committees a review of the activities of the Navy Cyber Warfare Development Group, including with respect to the authorities of the Group. The review shall include the following:

''(1) An assessment of whether such authorities shall be conferred on the 90th Cyberspace Operations Squadron of the Air Force.

''(2) A consideration of whether the 90th Cyberspace Operations Squadron should be designated a controlled tour, as defined by the Secretary.''

NOTIFICATION OF DELEGATION OF AUTHORITIES TO THE SECRETARY OF DEFENSE FOR MILITARY OPERATIONS IN CYBERSPACE

Pub. L. 116–92, div. A, title XVI, §1642, Dec. 20, 2019, 133 Stat. 1751, provided that:

''(a) IN GENERAL.—The Secretary of Defense shall provide written notification to the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate of the following:

''(1) Authorities delegated to the Secretary by the President for military operations in cyberspace that are otherwise held by the National Command Authority, not later than 15 days after any such delegation. A notification under this paragraph shall include a description of the authorities delegated to the Secretary.

''(2) Concepts of operations approved by the Secretary pursuant to delegated authorities described in paragraph (1), not later than 15 days after any such approval. A notification under this paragraph shall include the following:

''(A) A description of authorized activities to be conducted or planned to be conducted pursuant to such authorities.

''(B) The defined military objectives relating to such authorities.

''(C) A list of countries in which such authorities may be exercised.

''(D) A description of relevant orders issued by the Secretary in accordance with such authorities.

''(b) PROCEDURES.—

''(1) IN GENERAL.—The Secretary of Defense shall establish and submit to the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate procedures for complying with the requirements of subsection (a), consistent with the national security of the United States and the protection of operational integrity. The Secretary shall promptly notify such committees in writing of any changes to such procedures at least 14 days prior to the adoption of any such changes.

''(2) SUFFICIENCY.—The Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate shall ensure that committee procedures designed to protect from unauthorized disclosure classified information relating to national security of the United States are sufficient to protect the information that is submitted to such committees pursuant to this section.

''(3) NOTIFICATION IN EVENT OF UNAUTHORIZED DISCLOSURE.—In the event of an unauthorized disclosure of authorities covered by this section, the Secretary of Defense shall ensure, to the maximum extent practicable, that the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate are notified immediately. Notification under this paragraph may be verbal or written, but in the event of a verbal notification, a written notification signed by the Secretary shall be provided by not later than 48 hours after the provision of such verbal notification.''

ANNUAL MILITARY CYBERSPACE OPERATIONS REPORT

Pub. L. 116–92, div. A, title XVI, §1644, Dec. 20, 2019, 133 Stat. 1752, as amended by Pub. L. 118–31, div. A, title X, §1061(d), Dec. 22, 2023, 137 Stat. 399, provided that:

''(a) IN GENERAL.—Not later than March 1 of each year, the Secretary of Defense shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a written report summarizing all named military cyberspace effects operations conducted in the previous calendar year, including cyber effects conducted for either offensive or defensive purposes. Each such summary should be organized by adversarial country and should include the following for each named operation:

''(1) An identification of the objective and purpose.

''(2) Descriptions of the impacted countries, organizations, or forces, and nature of the impact.

''(3) A description of methodologies used for the cyber effects operation or cyber effects enabling operation.

''(4) An identification of the Cyber Mission Force teams, or other Department of Defense entity or units, that conducted such operation, and supporting teams, entities, or units.

''(5) An identification of the infrastructures on which such operations occurred.

''(6) A description of relevant legal, operational, and funding authorities.

''(7) Additional costs beyond baseline operations and maintenance and personnel costs directly associated with the conduct of the cyber effects operation or cyber effects enabling operation.

''(8) Any other matters the Secretary determines relevant.

''(b) CLASSIFICATION.—The Secretary of Defense shall provide each report required under subsection (a) at a classification level the Secretary determines appropriate.

''(c) LIMITATION.—This section does not apply to cyber-enabled military information support operations or military deception operations or cyber effects operations for which Congress has otherwise been provided notice.''

POLICY OF THE UNITED STATES ON CYBERSPACE, CYBERSECURITY, CYBER WARFARE, AND CYBER DETERRENCE

Pub. L. 115–232, div. A, title XVI, §1636, Aug. 13, 2018, 132 Stat. 2126, provided that:

''(a) IN GENERAL.—It shall be the policy of the United States, with respect to matters pertaining to cyberspace, cybersecurity, and cyber warfare, that the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities of foreign powers that target United States interests with the intent to—

''(1) cause casualties among United States persons or persons of United States allies;

''(2) significantly disrupt the normal functioning of United States democratic society or government (including attacks against critical infrastructure that could damage systems used to provide key services to the public or government);

''(3) threaten the command and control of the Armed Forces, the freedom of maneuver of the Armed Forces, or the industrial base or other infrastructure on which the United States Armed Forces rely to defend United States interests and commitments; or

''(4) achieve an effect, whether individually or in aggregate, comparable to an armed attack or imperil a vital interest of the United States.

''(b) RESPONSE OPTIONS.—In carrying out the policy set forth in subsection (a), the United States shall plan, develop, and, when appropriate, demonstrate response options to address the full range of potential cyber attacks on United States interests that could be conducted by potential adversaries of the United States.

''(c) DENIAL OPTIONS.—In carrying out the policy set forth in subsection (a) through response options developed pursuant to subsection (b), the United States shall, to the greatest extent practicable, prioritize the defensibility and resiliency against cyber attacks and malicious cyber activities described in subsection (a) of infrastructure critical to the political integrity, economic security, and national security of the United States.

''(d) COST-IMPOSITION OPTIONS.—In carrying out the policy set forth in subsection (a) through response options developed pursuant to subsection (b), the United States shall develop and, when appropriate, demonstrate, or otherwise make known to adversaries the existence of, cyber capabilities to impose costs on any foreign power targeting the United States or United States persons with a cyber attack or malicious cyber activity described in subsection (a).

''(e) MULTI-PRONG RESPONSE.—In carrying out the policy set forth in subsection (a) through response options developed pursuant to subsection (b), the United States shall leverage all instruments of national power.

''(f) UPDATE ON PRESIDENTIAL POLICY.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Aug. 13, 2018], the President shall transmit, in unclassified and classified forms, as appropriate, to the appropriate congressional committees a report containing an update to the report provided to the Congress on the policy of the United States on cyberspace, cybersecurity, and cyber warfare pursuant to section 1633 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 10 U.S.C. 130g note) [now 10 U.S.C. 394 note].

''(2) CONTENTS.—The report required under paragraph (1) shall include the following:

''(A) An assessment of the current posture in cyberspace, including assessments of—

''(i) whether past responses to major cyber attacks have had the desired deterrent effect; and

''(ii) how adversaries have responded to past United States responses.

''(B) Updates on the Administration's efforts in the development of—

''(i) cost imposition strategies;

''(ii) varying levels of cyber incursion and steps taken to date to prepare for the imposition of the consequences referred to in clause (i); and

''(iii) the Cyber Deterrence Initiative.

''(C) Information relating to the Administration's plans, including specific planned actions, regulations, and legislative action required, for—

''(i) advancing technologies in attribution, inherently secure technology, and artificial intelligence society-wide;

''(ii) improving cybersecurity in and cooperation with the private sector;

''(iii) improving international cybersecurity cooperation; and

''(iv) implementing the policy referred to in paragraph (1), including any realignment of government or government responsibilities required, writ large.

''(f) [probably should be ''(g)''] RULE OF CONSTRUCTION.—Nothing in this subsection may be construed to limit the authority of the President or Congress to authorize the use of military force.

''(g) [probably should be ''(h)''] DEFINITIONS.—In this section:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

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

''(B) the Permanent Select Committee on Intelligence of the House of Representatives;

''(C) the Select Committee on Intelligence of the Senate;

''(D) the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on the Judiciary of the House of Representatives; and

''(E) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, and the Committee on the Judiciary of the Senate.

''(2) FOREIGN POWER.—The term 'foreign power' has the meaning given such term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).''

Pub. L. 115–91, div. A, title XVI, §1633, Dec. 12, 2017, 131 Stat. 1738, provided that:

''(a) IN GENERAL.—The President shall—

''(1) develop a national policy for the United States relating to cyberspace, cybersecurity, and cyber warfare; and

''(2) submit to the appropriate congressional committees a report on the policy.

''(b) ELEMENTS.—The national policy required under subsection (a) shall include the following elements:

''(1) Delineation of the instruments of national power available to deter or respond to cyber attacks or other malicious cyber activities by a foreign power or actor that targets United States interests.

''(2) Available or planned response options to address the full range of potential cyber attacks on United States interests that could be conducted by potential adversaries of the United States.

''(3) Available or planned denial options that prioritize the defensibility and resiliency against cyber attacks and malicious cyber activities that are carried out against infrastructure critical to the political integrity, economic security, and national security of the United States.

''(4) Available or planned cyber capabilities that may be used to impose costs on any foreign power targeting the United States or United States persons with a cyber attack or malicious cyber activity.

''(5) Development of multi-prong response options, such as—

''(A) boosting the cyber resilience of critical United States strike systems (including cyber, nuclear, and non-nuclear systems) in order to ensure the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attack;

''(B) developing offensive cyber capabilities and specific plans and strategies to put at risk targets most valued by adversaries of the United States and their key decision makers; and

''(C) enhancing attribution capabilities and developing intelligence and offensive cyber capabilities to detect, disrupt, and potentially expose malicious cyber activities.

''(c) LIMITATION ON AVAILABILITY OF FUNDS.—

''(1) IN GENERAL.—Of the funds authorized to be appropriated by this Act [see Tables for classification] or otherwise made available for fiscal year 2018 for procurement, research, development, test and evaluation, and operations and maintenance, for the covered activities of the Defense Information Systems Agency, not more than 60 percent may be obligated or expended until the date on which the President submits to the appropriate congressional committees the report under subsection (a)(2).

''(2) COVERED ACTIVITIES DESCRIBED.—The covered activities referred to in paragraph (1) are the activities of the Defense Information Systems Agency in support of—

''(A) the White House Communication Agency; and

''(B) the White House Situation Support Staff.

''(d) DEFINITIONS.—In this section:

''(1) The term 'foreign power' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

''(2) The term 'appropriate congressional committees' means—

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

''(B) the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on the Judiciary of the House of Representatives; and

''(C) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, and the Committee on the Judiciary of the Senate.''

ACTIVE DEFENSE AGAINST THE RUSSIAN FEDERATION, PEOPLE'S REPUBLIC OF CHINA, DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA, AND ISLAMIC REPUBLIC OF IRAN ATTACKS IN CYBERSPACE

Pub. L. 115–232, div. A, title XVI, §1642, Aug. 13, 2018, 132 Stat. 2132, provided that:

''(a) AUTHORITY TO DISRUPT, DEFEAT, AND DETER CYBER ATTACKS.—

''(1) IN GENERAL.—In the event that the National Command Authority determines that the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, or Islamic Republic of Iran is conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes, the National Command Authority may authorize the Secretary of Defense, acting through the Commander of the United States Cyber Command, to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter such attacks under the authority and policy of the Secretary of Defense to conduct cyber operations and information operations as traditional military activities.

''(2) NOTIFICATION AND REPORTING.—

''(A) NOTIFICATION OF OPERATIONS.—In exercising the authority provided in paragraph (1), the Secretary shall provide notices to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] in accordance with section 395 of title 10, United States Code (as transferred and redesignated pursuant to section 1631).

''(B) QUARTERLY REPORTS BY COMMANDER OF THE UNITED STATES CYBER COMMAND.—

''(i) IN GENERAL.—In any fiscal year in which the Commander of the United States Cyber Command carries out an action under paragraph (1), the Secretary of Defense shall, not less frequently than quarterly, submit to the congressional defense committees a report on the actions of the Commander under such paragraph in such fiscal year.

''(ii) MANNER OF REPORTING.—Reports submitted under clause (i) shall be submitted in a manner that is consistent with the recurring quarterly report required by section 484 of title 10, United States Code.

''(b) PRIVATE SECTOR COOPERATION.—The Secretary may make arrangements with private sector entities, on a voluntary basis, to share threat information related to malicious cyber actors, and any associated false online personas or compromised infrastructure, associated with a determination under subsection (a)(1), consistent with the protection of sources and methods and classification guidelines, as necessary.

''(c) ANNUAL REPORT.—Not less frequently than once each year, the Secretary shall submit to the congressional defense committees, the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), the Committee on Foreign Affairs of the House of Representatives, and the Committee on Foreign Relations of the Senate a report on—

''(1) the scope and intensity of the information operations and attacks through cyberspace by the countries specified in subsection (a)(1) against the government or people of the United States observed by the cyber mission forces of the United States Cyber Command and the National Security Agency; and

''(2) adjustments of the Department of Defense in the response directed or recommended by the Secretary with respect to such operations and attacks.

''(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

''(1) limit the authority of the Secretary to conduct military activities or operations in cyberspace, including clandestine activities or operations in cyberspace; or

''(2) affect the War Powers Resolution (Public Law 93–148; 50 U.S.C. 1541 et seq.) or the Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note).''

PILOT PROGRAM TO MODEL CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

Pub. L. 115–232, div. A, title XVI, §1649, Aug. 13, 2018, 132 Stat. 2137, provided that:

''(a) PILOT PROGRAM REQUIRED.—

''(1) IN GENERAL.—The Assistant Secretary of Defense for Homeland Defense and Global Security shall carry out a pilot program to model cyber attacks on critical infrastructure in order to identify and develop means of improving Department of Defense responses to requests for defense support to civil authorities for such attacks.

''(2) RESEARCH EXERCISES.—The pilot program shall source data from and include consideration of the

'Jack Voltaic' research exercises conducted by the Army Cyber Institute, industry partners of the Institute, and the cities of New York, New York, and Houston, Texas.

''(b) PURPOSE.—The purpose of the pilot program shall be to accomplish the following:

''(1) The development and demonstration of risk analysis methodologies, and the application of commercial simulation and modeling capabilities, based on artificial intelligence and hyperscale cloud computing technologies, as applicable—

''(A) to assess defense critical infrastructure vulnerabilities and interdependencies to improve military resiliency;

''(B) to determine the likely effectiveness of attacks described in subsection (a)(1), and countermeasures, tactics, and tools supporting responsive military homeland defense operations;

''(C) to train personnel in incident response;

''(D) to conduct exercises and test scenarios;

''(E) to foster collaboration and learning between and among departments and agencies of the Federal Government, State and local governments, and private entities responsible for critical infrastructure; and

''(F) improve intra-agency and inter-agency coordination for consideration and approval of requests for defense support to civil authorities.

''(2) The development and demonstration of the foundations for establishing and maintaining a program of record for a shared high-fidelity, interactive, affordable, cloud-based modeling and simulation of critical infrastructure systems and incident response capabilities that can simulate complex cyber and physical attacks and disruptions on individual and multiple sectors on national, regional, State, and local scales.

''(c) REPORT.—

''(1) IN GENERAL.—At the same time the budget of the President for fiscal year 2021 is submitted to Congress pursuant to section 1105(a) of title 31, United States Code, the Assistant Secretary shall, in consultation with the Secretary of Homeland Security, submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the pilot program.

''(2) CONTENTS.—The report required by paragraph (1) shall include the following:

''(A) A description of the results of the pilot program as of the date of the report.

''(B) A description of the risk analysis methodologies and modeling and simulation capabilities developed and demonstrated pursuant to the pilot program, and an assessment of the potential for future growth of commercial technology in support of the homeland defense mission of the Department of Defense.

''(C) Such recommendations as the Secretary considers appropriate regarding the establishment of a program of record for the Department on further development and sustainment of risk analysis methodologies and advanced, large-scale modeling and simulation on critical infrastructure and cyber warfare.

''(D) Lessons learned from the use of novel risk analysis methodologies and large-scale modeling and simulation carried out under the pilot program regarding vulnerabilities, required capabilities, and reconfigured force structure, coordination practices, and policy.

''(E) Planned steps for implementing the lessons described in subparagraph (D).

''(F) Any other matters the Secretary determines appropriate.''

IDENTIFICATION OF COUNTRIES OF CONCERN REGARDING CYBERSECURITY

Pub. L. 115–232, div. A, title XVI, §1654, Aug. 13, 2018, 132 Stat. 2148, provided that:

''(a) IDENTIFICATION OF COUNTRIES OF CONCERN.—Not later than 180 days after the date of the enactment of this Act [Aug. 13, 2018], the Secretary of Defense shall create a list of countries that pose a risk to the cybersecurity of United States defense and national security systems and infrastructure. Such list shall reflect the level of threat posed by each country included on such list. In creating such list, the Secretary shall take in to account the following:

''(1) A foreign government's activities that pose force protection or cybersecurity risk to the personnel, financial systems, critical infrastructure, or information systems of the United States or coalition forces.

''(2) A foreign government's willingness and record of providing financing, logistics, training or intelligence to other persons, countries or entities posing a force protection or cybersecurity risk to the personnel, financial systems, critical infrastructure, or information systems of the United States or coalition forces.

''(3) A foreign government's engagement in foreign intelligence activities against the United States for the purpose of undermining United States national security.

''(4) A foreign government's knowing participation in transnational organized crime or criminal activity.

''(5) A foreign government's cyber activities and operations to affect the supply chain of the United States Government.

''(6) A foreign government's use of cyber means to unlawfully or inappropriately obtain intellectual property from the United States Government or United States persons.

''(b) UPDATES.—The Secretary shall continuously update and maintain the list under subsection (a) to preempt obsolescence.

''(c) REPORT TO CONGRESS.—Not later than one year after the date of the enactment of this Act, the Secretary shall submit to the appropriate committees of Congress the list created pursuant to subsection (a) and any accompanying analysis that contributed to the creation of the list.''

QUADRENNIAL COMPREHENSIVE CYBER POSTURE REVIEW

Pub. L. 115–91, div. A, title XVI, §1644, Dec. 12, 2017, 131 Stat. 1748, as amended by Pub. L. 116–92, div. A, title XVI, §1635, Dec. 20, 2019, 133 Stat. 1748; Pub. L. 116–283, div. A, title XVII, §1706, Jan. 1, 2021, 134 Stat. 4083, provided that:

''(a) REQUIREMENT FOR COMPREHENSIVE REVIEW.—In order to clarify the near-term policy and strategy of the United States with respect to cyber deterrence, the Secretary of Defense shall, not later than December 31, 2022, and quadrennially thereafter, conduct a comprehensive review of the cyber posture of the United States over the posture review period.

''(b) CONSULTATION.—The Secretary of Defense shall conduct each review under subsection (a) in consultation with the Director of National Intelligence, the Attorney General, the Secretary of Homeland Security, and the Secretary of State, as appropriate.

''(c) ELEMENTS OF REVIEW.—Each review conducted under subsection (a) shall include, for the posture review period, the following elements:

''(1) The assessment and definition of the role of cyber forces in the national defense and military strategies of the United States.

''(2) Review of the following:

''(A) The role of cyber operations in combatant commander warfighting plans.

''(B) The ability of combatant commanders to respond to adversary cyber attacks.

''(C) The international partner cyber capacity-building programs of the Department.

''(3) A review of the law, policies, and authorities relating to, and necessary for, the United States to maintain a safe, reliable, and credible cyber posture for defending against and responding to cyber attacks

and for deterrence in cyberspace, including the following:

''(A) An assessment of the need for further delegation of cyber-related authorities, including those germane to information warfare, to the Commander of United States Cyber Command.

''(B) An evaluation of the adequacy of mission authorities for all cyber-related military components, defense agencies, directorates, centers, and commands.

''(4) A review of the need for or for updates to a declaratory policy relating to the responses of the United States to cyber attacks of significant consequence.

''(5) A review of norms for the conduct of offensive cyber operations for deterrence and in crisis and conflict.

''(6) A review of a strategy to deter, degrade, or defeat malicious cyber activity targeting the United States (which may include activities, capability development, and operations other than cyber activities, cyber capability development, and cyber operations), including—

''(A) a review and assessment of various approaches to competition and deterrence in cyberspace, determined in consultation with experts from Government, academia, and industry;

''(B) a comparison of the strengths and weaknesses of the approaches identified pursuant to subparagraph (A) relative to the threat of each other; and

''(C) an assessment as to how the cyber strategy will inform country-specific campaign plans focused on key leadership of Russia, China, Iran, North Korea, and any other country the Secretary considers appropriate.

''(7) Identification of the steps that should be taken to bolster stability in cyberspace and, more broadly, stability between major powers, taking into account—

''(A) the analysis and gaming of escalation dynamics in various scenarios; and

''(B) consideration of the spiral escalatory effects of countries developing increasingly potent offensive cyber capabilities.

''(8) A comprehensive force structure assessment of the Cyber Operations Forces of the Department for the posture review period, including the following:

''(A) A determination of the appropriate size and composition of the Cyber Mission Forces to accomplish the mission requirements of the Department.

''(B) An assessment of the Cyber Mission Forces' personnel, capabilities, equipment, funding, operational concepts, and ability to execute cyber operations in a timely fashion.

''(C) An assessment of the personnel, capabilities, equipment, funding, and operational concepts of Cybersecurity Service Providers and other elements of the Cyber Operations Forces.

''(9) An assessment of whether the Cyber Mission Force has the appropriate level of interoperability, integration, and interdependence with special operations and conventional forces.

''(10) An evaluation of the adequacy of mission authorities for the Joint Force Provider and Joint Force Trainer responsibilities of United States Cyber Command, including the adequacy of the units designated as Cyber Operations Forces to support such responsibilities.

''(11) An assessment of the missions and resourcing of the combat support agencies in support of cyber missions of the Department.

''(12) An assessment of the potential costs, benefits, and value, if any, of establishing a cyber force as a separate uniformed service.

''(13) Any recurrent problems or capability gaps that remain unaddressed since the previous posture review.

''(14) Such other matters as the Secretary considers appropriate.

''(d) REPORT.—

''(1) IN GENERAL.—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 report on the results of each cyber posture review conducted under subsection (a).

''(2) FORM OF REPORT.—Each report under paragraph (1) may be submitted in unclassified form or classified form, as necessary.

''(e) POSTURE REVIEW PERIOD DEFINED.—In this section, the term 'posture review period' means the eight-year period that begins on the date of each review conducted under subsection (a).''

§ 395. Notification requirements for sensitive military cyber operations

(a) IN GENERAL.—Except as provided in subsection (d), the Secretary of Defense shall promptly submit to the congressional defense committees notice in writing of any sensitive military cyber operation conducted under this title no later than 48 hours following such operation.

(b) PROCEDURES.—(1) The Secretary of Defense shall establish and submit to the congressional defense committees procedures for complying with the requirements of subsection (a) consistent with the national security of the United States and the protection of operational integrity. The Secretary shall promptly notify the congressional defense committees in writing of any changes to such procedures at least 14 days prior to the adoption of any such changes.

(2) The congressional defense committees shall ensure that committee procedures designed to protect from unauthorized disclosure classified information relating to national security of the United States are sufficient to protect the information that is submitted to the committees pursuant to this section.

(3) In the event of an unauthorized disclosure of a sensitive military cyber operation covered by this section, the Secretary shall ensure, to the maximum extent practicable, that the congressional defense committees are notified immediately of the sensitive military cyber operation concerned. The notification under this paragraph may be verbal or written, but in the event of a verbal notification a written notification, signed by the Secretary, or the Secretary's designee, shall be provided by not later than 48 hours after the provision of the verbal notification.

(c) SENSITIVE MILITARY CYBER OPERATION DEFINED.—(1) In this section, the term ''sensitive military cyber operation'' means an action described in paragraph (2) that—

(A) is carried out by the armed forces of the United States;

(B) is intended to achieve a cyber effect against a foreign terrorist organization or a country, including its armed forces and the proxy forces of that country located elsewhere—

(i) with which the armed forces of the United States are not involved in hostilities (as that term is used in section 4 of the War Powers Resolution (50 U.S.C. 1543)); or

(ii) with respect to which the involvement of the armed forces of the United States in hostilities has not been acknowledged publicly by the United States; and