Subtitle C—Cyberspace-Related Matters

PART I—GENERAL CYBER MATTERS

SEC. 1631. NOTIFICATION REQUIREMENTS FOR SENSITIVE MILITARY CYBER OPERATIONS AND CYBER WEAPONS.

(a) NOTIFICATION.—Chapter 3 of title 10, United States Code, is amended by adding at the end the following new sections:

"§ 130j. 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 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; and

"(B) is intended to cause cyber effects outside a geographic location—

"(i) where the armed forces of the United States are involved in hostilities (as that term is used in section 1543 of title 50, United States Code); or

"(ii) with respect to which hostilities have been declared by the United States.

"(2) The actions described in this paragraph are the following:

"(A) An offensive cyber operation.

"(B) A defensive cyber operation outside the Department of Defense Information Networks to defeat an ongoing or imminent threat.

"(d) EXCEPTIONS.—The notification requirement under subsection (a) does not apply—

"(1) to a training exercise conducted with the consent of all nations where the intended effects of the exercise will occur; or

"(2) to a covert action (as that term is defined in section 3093 of title 50, United States Code).

"(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide any new authority 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 any requirement under the National Security Act of 1947 (50 U.S.C. 3001 et seq.).

"§ 130k. Notification requirements for cyber weapons

"(a) IN GENERAL.—Except as provided in subsection (c), the Secretary of Defense shall promptly submit to the congressional defense committees notice in writing of the following:

"(1) With respect to a cyber capability that is intended for use as a weapon, on a quarterly basis, the aggregated results of all reviews of the capability for legality under international law pursuant to Department of Defense Directive 5000.01 carried out by any military department concerned.

"(2) The use as a weapon of any cyber capability that has been approved for such use under international law by a military department no later than 48 hours following such use.

"(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 cyber capability covered by this section, the Secretary shall ensure, to the maximum extent practicable, that the congressional defense committees are notified immediately of the cyber capability concerned. The notification under this paragraph may be verbal or written, but in the event of a verbal notification a written notification shall be provided by not later than 48 hours after the provision of the verbal notification.

"(c) EXCEPTIONS.—The notification requirement under subsection (a) does not apply—

"(1) to a training exercise conducted with the consent of all nations where the intended effects of the exercise will occur; or

"(2) to a covert action (as that term is defined in section 3093 of title 50, United States Code).

"(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide any new authority 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 any requirement under the National Security Act of 1947 (50 U.S.C. 3001 et seq.).".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by adding at the end the following new items:

"130j. Notification requirements for sensitive military cyber operations
"130k. Notification requirements for cyber weapons".

SEC. 1632. MODIFICATION TO QUARTERLY CYBER OPERATIONS BRIEFINGS.

(a) IN GENERAL.—Section 484 of title 10, United States Code, is amended—

(1) by striking "The Secretary of Defense shall provide to the Committees on Armed Services of the House of Representatives and the Senate" and inserting the following:

"(a) BRIEFINGS REQUIRED.—The Secretary of Defense shall provide to the congressional defense committees"; and

(2) by adding at the end the following:

"(b) ELEMENTS.—Each briefing under subsection (a) shall include, with respect to the military operations in cyberspace described in such subsection, the following:

"(1) An update, set forth separately for each geographic and functional command, that describes the operations carried out by the command and any hostile cyber activity directed at the command.

"(2) An overview of authorities and legal issues applicable to the operations, including any relevant legal limitations.

"(3) An outline of any interagency activities and initiatives relating to the operations.

"(4) Any other matters the Secretary determines to be appropriate.".

(b) EFFECTIVE DATE.—The amendments made by subsection (a) shall take effect on the date of the enactment of this Act, and shall apply with respect to briefings required be provided under section 484 of title 10, United States Code, on or after that date.

SEC. 1633. POLICY OF THE UNITED STATES ON CYBERSPACE, CYBERSECURITY, AND CYBER WARFARE.

(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 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;

(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.

SEC. 1634. PROHIBITION ON USE OF PRODUCTS AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB.

(a) PROHIBITION.—No department, agency, organization, or other element of the Federal Government may use, whether directly or through work with or on behalf of another department, agency, organization, or element of the Federal Government, any hardware, software, or services developed or provided, in whole or in part, by—

(1) Kaspersky Lab (or any successor entity);

(2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(3) any entity of which Kaspersky Lab has majority ownership.

(b) EFFECTIVE DATE.—The prohibition in subsection (a) shall take effect on October 1, 2018.

(c) REVIEW AND REPORT.—

(1) REVIEW.—The Secretary of Defense, in consultation with the Secretary of Energy, the Secretary of Homeland Security, the Attorney General, the Administrator of the General Services Administration, and the Director of National Intelligence, shall conduct a review of the procedures for removing suspect products or services from the information technology networks of the Federal Government.

(2) REPORT.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, Secretary of Defense shall submit to the appropriate congressional committees a report on the review conducted under paragraph (1).

(B) ELEMENTS.—The report under subparagraph (A) shall include the following:

(i) A description of the Federal Government-wide authorities that may be used to prohibit, exclude, or prevent the use of suspect products or services on the information technology networks of the Federal Government, including—

(I) the discretionary authorities of agencies to prohibit, exclude, or prevent the use of such products or services;

(II) the authorities of a suspension and debarment official to prohibit, exclude, or prevent the use of such products or services;

(III) authorities relating to supply chain risk management;

(IV) authorities that provide for the continuous monitoring of information technology networks to identify suspect products or services; and

(V) the authorities provided under the Federal Information Security Management Act of 2002.

(ii) Assessment of any gaps in the authorities described in clause (i), including any gaps in the enforcement of decisions made under such authorities.

(iii) An explanation of the capabilities and methodologies used to periodically assess and monitor the information technology networks of the Federal Government for prohibited products or services.

(iv) An assessment of the ability of the Federal Government to periodically conduct training and exercises in the use of the authorities described in clause (i)—

(I) to identify recommendations for streamlining process; and

(II) to identify recommendations for education and training curricula, to be integrated into existing training or certification courses.

(v) A description of information sharing mechanisms that may be used to share information about suspect products or services, including mechanisms for the sharing of such information among the Federal Government, industry, the public, and international partners.

(vi) Identification of existing tools for business intelligence, application management, and commerce due-diligence that are either in use by elements of the Federal Government, or that are available commercially.

(vii) Recommendations for improving the authorities, processes, resourcing, and capabilities of the Federal Government for the purpose of improving the procedures for identifying and removing prohibited products or services from the information technology networks of the Federal Government.

(viii) Any other matters the Secretary determines to be appropriate.

(C) FORM.—The report under subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term "appropriate congressional committees" means the following:

(A) The Committee on Armed Services, the Committee on Energy and Commerce, the Committee on Homeland Security, the Committee on the Judiciary, the Committee on Oversight and Government Reform, and the Permanent Select Committee on Intelligence of the House of Representatives.

(B) The Committee on Armed Services, the Committee on Energy and Natural Resources, the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, and the Select Committee on Intelligence of the Senate.

SEC. 1635. MODIFICATION OF AUTHORITIES RELATING TO ESTABLISHMENT OF UNIFIED COMBATANT COMMAND FOR CYBER OPERATIONS.

Section 167b of title 10, United States Code, is amended—

(1) by striking subsection (d); and

(2) by redesignating subsections (e) and (f) as subsections (d) and (e), respectively.

SEC. 1636. MODIFICATION OF DEFINITION OF ACQUISITION WORKFORCE TO INCLUDE PERSONNEL CONTRIBUTING TO CYBERSECURITY SYSTEMS.

Section 1705(h)(2)(A) of title 10, United States Code, is amended—

(1) by inserting "(i)" after "(A)";

(2) by striking "; and" and inserting "; or"; and

(3) by adding at the end the following new clause:

"(ii) contribute significantly to the acquisition or development of systems relating to cybersecurity; and".

SEC. 1637. INTEGRATION OF STRATEGIC INFORMATION OPERATIONS AND CYBER-ENABLED INFORMATION OPERATIONS.

(a) PROCESSES AND PROCEDURES FOR INTEGRATION.—

(1) IN GENERAL.—The Secretary of Defense shall—

(A) establish processes and procedures to integrate strategic information operations and cyber-enabled information operations across the elements of the Department of Defense responsible for such operations, including the elements of the Department responsible for military deception, public affairs, electronic warfare, and cyber operations; and

(B) ensure that such processes and procedures provide for integrated Defense-wide strategy, planning, and budgeting with respect to the conduct of such operations by the Department, including activities conducted to counter and deter such operations by malign actors.

(2) DESIGNATED SENIOR OFFICIAL.—The Secretary of Defense shall designate a senior official of the Department of Defense (in this section referred to as the "designated senior official") who shall implement and oversee the processes and procedures established under paragraph (1). The designated senior official shall be selected by the Secretary from among individuals serving in the Department of Defense at or below the level of an Under Secretary of Defense.

(3) RESPONSIBILITIES.—The designated senior official shall have, with respect to the implementation and oversight of the processes and procedures established under paragraph (1), the following responsibilities:

(A) Oversight of strategic policy and guidance.

(B) Overall resource management for the integration of information operations and cyber-enabled information operations of the Department.

(C) Coordination with the head of the Global Engagement Center to support the purpose of the Center (as described section 1287(a)(2) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 22 U.S.C. 2656 note)) and liaison with the Center and other relevant Federal Government entities to support such purpose.

(D) Development of a strategic framework for the conduct of information operations by the Department of Defense, including cyber-enabled information operations, coordinated across all relevant elements of the Department of Defense, including both near-term and long-term guidance for the conduct of such coordinated operations.

(E) Development and dissemination of a common operating paradigm across the elements of the Department of Defense specified in paragraph (1) to counter the influence, deception, and propaganda activities of key malign actors, including in cyberspace.

(F) Development of guidance for, and promotion of, the capability of the Department of Defense to liaison with the private sector, including social media, on matters relating to the influence activities of malign actors.

(b) REQUIREMENTS AND PLANS FOR INFORMATION OPERATIONS.—

(1) COMBATANT COMMAND PLANNING AND REGIONAL STRATEGY.—(A) The Secretary shall require each commander

of a combatant command to develop, in coordination with the relevant regional Assistant Secretary of State or Assistant Secretaries of State and with the assistance of the Coordinator of the Global Engagement Center and the designated senior official, a regional information strategy and interagency coordination plan for carrying out the strategy, where applicable.

(B) The Secretary shall require each commander of a combatant command to develop such requirements and specific plans as may be necessary for the conduct of information operations in support of the strategy required under subparagraph (A), including plans for deterring information operations, including deterrence in the cyber domain, by malign actors against the United States, allies of the United States, and interests of the United States.

(2) IMPLEMENTATION PLAN FOR DOD STRATEGY FOR OPERATIONS IN THE INFORMATION ENVIRONMENT.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the designated senior official shall—

(i) review the strategy of the Department of Defense titled "Department of Defense Strategy for Operations in the Information Environment" and dated June 2016; and

(ii) submit to the congressional defense committees a plan for implementation of such strategy.

(B) ELEMENTS.—The plan required under subparagraph (A) shall include, at a minimum, the following:

(i) An accounting of the efforts undertaken in support of the strategy described in subparagraph (A)(i) in the period since it was issued in June 2016.

(ii) A description of any updates or changes to such strategy that have been made since it was first issued, as well as any expected updates or changes resulting from the designation of the designated senior official.

(iii) A description of the role of the Department of Defense as part of a broader whole-of-Government strategy for strategic communications, including a description of any assumptions about the roles and contributions of other departments and agencies of the Federal Government with respect to such a strategy.

(iv) Defined actions, performance metrics, and projected timelines for achieving each of the 15 tasks specified in the strategy described in subparagraph (A)(i).

(v) An analysis of any personnel, resourcing, capability, authority, or other gaps that will need to be addressed to ensure effective implementation of the strategy described in subparagraph (A)(i) across all relevant elements of the Department of Defense.

(vi) An investment framework and projected timeline for addressing any gaps identified under clause (v).

(vii) Such other matters as the Secretary of Defense considers relevant.

(C) PERIODIC STATUS REPORTS.—Not less frequently than once every 90 days during the three-year period beginning on the date on which the implementation plan is submitted under subparagraph (A)(ii), the designated senior official shall submit to the congressional defense committees a report describing the status of the efforts of the Department of Defense in accomplishing the tasks specified under clauses (iv) and (vi) of subparagraph (B).

(c) TRAINING AND EDUCATION.—Consistent with the elements of the implementation plan under paragraph (2), the designated senior official shall recommend the establishment of programs to provide training and education to such members of the Armed Forces and civilian employees of the Department of Defense as the Secretary considers appropriate to ensure that such members and employees understand the role of information in warfare, the central goal of all military operations to affect the perceptions, views, and decision making of adversaries, and the effective management and conduct of operations in the information environment.

SEC. 1638. EXERCISE ON ASSESSING CYBERSECURITY SUPPORT TO ELECTION SYSTEMS OF STATES.

(a) INCLUSION OF CYBER VULNERABILITIES IN ELECTION SYSTEMS IN CYBER GUARD EXERCISES.—Subject to subsection (b), the Secretary of Defense, in consultation with the Secretary of Homeland Security, may carry out exercises relating to the cybersecurity of election systems of States as part of the exercise commonly known as the "Cyber Guard Exercise".

(b) AGREEMENT REQUIRED.—The Secretary of Defense may carry out an exercise relating to the cybersecurity of a State's election system under subsection (a) only if the State enters into a written agreement with the Secretary under which the State—

(1) agrees to participate in such exercise; and

(2) agrees to allow vulnerability testing of the components of the State's election system.

(c) REPORT.—Not later than 90 days after the completion of any Cyber Guard Exercise, the Secretary of Defense shall submit to the congressional defense committees a report on the ability of the National Guard to assist States, if called upon, in defending election systems from cyberattacks. Such report shall include a description of the capabilities, readiness levels, and best practices of the National Guard with respect to the prevention of cyber attacks on State election systems.

SEC. 1639. MEASUREMENT OF COMPLIANCE WITH CYBERSECURITY REQUIREMENTS FOR INDUSTRIAL CONTROL SYSTEMS.

(a) IN GENERAL.—Not later than January 1, 2018, the Secretary of Defense shall make such changes to the cybersecurity scorecard as are necessary to ensure that the Secretary measures the progress of each element of the Department of Defense in securing the industrial control systems of the Department against cyber threats, including such industrial control systems as supervisory control and data acquisition systems, distributed control systems, programmable logic controllers, and platform information technology.

(b) CYBERSECURITY SCORECARD DEFINED.—In this section, the term "cybersecurity scorecard" means the Department of Defense Cybersecurity Scorecard used by the Department to measure compliance with cybersecurity requirements as described in the plan of

the Department titled "Department of Defense Cybersecurity Discipline Implementation Plan".

SEC. 1640. STRATEGIC CYBERSECURITY PROGRAM.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, in consultation with the Director of the National Security Agency, shall submit to the congressional defense committees a plan for the establishment of a program to be known as the "Strategic Cybersecurity Program" or "SCP" (in this section referred to as the "Program").

(b) ELEMENTS.—The Program shall be comprised of personnel assigned to the Program by the Secretary of Defense from among personnel, including regular and reserve members of the Armed Forces, civilian employees of the Department, and personnel of the research laboratories of the Department of Defense and the Department of Energy, who have particular expertise in the areas of responsibility described in subsection (c). Any personnel assigned to the Program from among personnel of the Department of Energy shall be so assigned with the concurrence of the Secretary of Energy.

(c) RESPONSIBILITIES.—

(1) IN GENERAL.—Personnel assigned to the Program shall assist the Department of Defense in improving the cybersecurity of the following systems of the Federal Government:

(A) Offensive cyber systems.

(B) Long-range strike systems.

(C) Nuclear deterrent systems.

(D) National security systems.

(E) Critical infrastructure of the Department of Defense (as that term is defined in section 1650(f)(1) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 10 U.S.C. 2224 note)).

(2) REVIEWS OF SYSTEMS AND INFRASTRUCTURE.—In carrying out the activities described in paragraph (1), the personnel assigned to the Program shall conduct appropriate reviews of existing systems and infrastructure and acquisition plans for proposed systems and infrastructure. The review of an acquisition plan for any proposed system or infrastructure shall be carried out before Milestone B approval for such system or infrastructure.

(3) RESULTS OF REVIEWS.—The results of each review carried out under paragraph (2), including any remedial action recommended pursuant to such review, shall be made available to any agencies or organizations of the Department involved in the development, procurement, operation, or maintenance of the system or infrastructure concerned.

(d) INTEGRATION WITH OTHER EFFORTS.—The plan required under subsection (a) shall build upon, and shall not duplicate, other efforts of the Department of Defense relating to cybersecurity, including—

(1) the evaluation of cyber vulnerabilities of major weapon systems of the Department of Defense required under section 1647 of the National Defense Authorization Act for Fiscal Year 2016 (114–92; 129 Stat. 1118);

(2) the evaluation of cyber vulnerabilities of Department of Defense critical infrastructure required under section 1650 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 10 U.S.C. 2224 note); and

(3) the activities of the cyber protection teams of the Department of Defense.

(e) REPORT.—Not later than one year after the date on which the plan is submitted to the congressional defense committees under subsection (a), the Secretary of Defense shall submit to the congressional defense committees a report on any activities carried out pursuant to such plan. The report shall include the following:

(1) A description of any activities of the Program carried out pursuant to the plan during the time period covered by the report.

(2) A description of particular challenges encountered in the course of the activities of the Program, if any, and of actions taken to address such challenges.

(3) A description of any plans for additional activities under the Program.

SEC. 1641. PLAN TO INCREASE CYBER AND INFORMATION OPERATIONS, DETERRENCE, AND DEFENSE.

(a) PLAN.—The Secretary of Defense shall develop a plan to—

(1) increase inclusion of regional cyber planning within larger joint planning exercises of the United States in the Indo-Asia-Pacific region;

(2) enhance joint, regional, and combined information operations and strategic communication strategies to counter Chinese and North Korean information warfare, malign influence, and propaganda activities; and

(3) identify potential areas of cybersecurity collaboration and partnership capabilities with Asian allies and partners of the United States.

(b) BRIEFING.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall provide to the congressional defense committees a briefing on the plan required under subsection (a).

SEC. 1642. EVALUATION OF AGILE OR ITERATIVE DEVELOPMENT OF CYBER TOOLS AND APPLICATIONS.

(a) EVALUATION REQUIRED.—The Commander of the United States Cyber Command (in this section referred to as the "Commander") shall conduct an evaluation of alternative methods for developing, acquiring, and maintaining software-based cyber tools and applications for the United States Cyber Command, the Army Cyber Command, the Fleet Cyber Command, the Air Force Cyber Command, and the Marine Corps Cyberspace Command.

(b) GOAL.—The goal of the evaluation required by subsection (a) shall be to identify a set of practices that will—

(1) increase the speed of development of cyber capabilities of the Armed Forces;

(2) provide more effective tools and capabilities for developing, acquiring, and maintaining software-based cyber tools and applications for the Armed Forces; and

(3) create a repeatable, disciplined process for developing, acquiring, and maintaining software-based cyber tools and applications for the Armed Forces through which progress and success or failure can be continuously measured.

(c) CONSIDERATION OF AGILE OR ITERATIVE DEVELOPMENT, AND OTHER BEST PRACTICES.—

(1) IN GENERAL.—The evaluation required by subsection (a) shall include, with respect to the development, acquisition,

and maintenance of software-based cyber tools and applications, consideration of agile or iterative development practices, agile acquisition practices, and other similar best practices of commercial industry.

(2) CONSIDERATIONS.—In carrying out the evaluation required by subsection (a), the Commander shall assess requirements for implementing the practices described in paragraph (1) and consider changes to established acquisition practices that may be necessary to implement the practices described in such paragraph, including changes to the following:

(A) The requirements process.

(B) Contracting.

(C) Testing.

(D) User involvement in the development process.

(E) Program management.

(F) Milestone reviews and approvals.

(G) The definitions of "research and development", "procurement", and "sustainment".

(H) The constraints of current appropriations account definitions.

(d) ASSESSMENT OF TRAINING AND EDUCATION REQUIREMENTS.—In carrying out the evaluation required by subsection (a), the Commander shall assess training and education requirements for personnel in all areas and at all levels of management relevant to the successful adoption of new acquisition models and methods for developing, acquiring, and maintaining cyber tools and applications as described in such subsection.

(e) SERVICES AND EXPERTISE.—In carrying out the evaluation required by subsection (a), the Commander shall—

(1) obtain services and expertise from—

(A) the Defense Digital Service; and

(B) federally funded research and development centers, such as the Software Engineering Institute and the MITRE Corporation; and

(2) consult with such commercial software companies as the Commander considers appropriate to learn about relevant commercial best practices.

(f) RECOMMENDATIONS.—

(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Commander shall submit to the Secretary of Defense recommendations for experimenting with or adopting new acquisition methods identified pursuant to the evaluation under subsection (a), including recommendations for any actions that should be carried out to ensure the successful implementation of such methods.

(2) CONGRESSIONAL BRIEFING.—Not later than 14 days after submitting recommendations to the Secretary under paragraph (1), the Commander shall provide to the congressional defense committees a briefing on the recommendations.

(g) PRESERVATION OF EXISTING AUTHORITY.—The evaluation required under subsection (a) is intended to inform future acquisition approaches. Nothing in this section shall be construed to limit or impede the Commander in exercising the authority provided under section 807 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 10 U.S.C. 2224 note).

(h) AGILE OR ITERATIVE DEVELOPMENT DEFINED.—In this section, the term "agile or iterative development", with respect to software—

(1) means acquisition pursuant to a method for delivering multiple, rapid, incremental capabilities to the user for operational use, evaluation, and feedback not exclusively linked to any single, proprietary method or process; and

(2) involves—

(A) the incremental development and fielding of capabilities, commonly called "spirals", "spins", or "sprints", which can be measured in a few weeks or months; and

(B) continuous participation and collaboration by users, testers, and requirements authorities.

SEC. 1643. ASSESSMENT OF DEFENSE CRITICAL ELECTRIC INFRASTRUCTURE.

Section 1650(b)(1) of the National Defense Authorization Act for fiscal year 2017 (114–328; 10 U.S.C. 2224 note) is amended—

(1) in subparagraph (C), by striking "and" at the end;

(2) in subparagraph (D), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following:

"(E) to assess the strategic benefits derived from, and the challenges associated with, isolating military infrastructure from the national electric grid and the use of microgrids.".

SEC. 1644. CYBER POSTURE REVIEW.

(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 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 the 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.—The review conducted under subsection (a) shall include, for the posture review period, the following elements:

(1) The role of cyber forces in the military strategy, planning, and programming of the United States.

(2) Review of the role of cyber operations in combatant commander operational planning, the ability of combatant commanders to respond to hostile acts by adversaries, and the ability of combatant commanders to engage and build capacity with allies.

(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 responding to cyber attacks and for deterrence in cyberspace.

(4) A declaratory policy relating to the responses of the United States to cyber attacks of significant consequence.

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

(6) Guidance for the development of a cyber deterrence strategy (which may include activities, capability efforts, and

operations other than cyber activities, cyber capability efforts, and cyber operations), including—

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

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

(C) an explanation of how the cyber deterrence strategy will inform country-specific deterrence 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 determination of whether sufficient personnel are trained and equipped to meet validated cyber requirements.

(9) Such other matters as the Secretary considers appropriate.

(d) REPORT.—

(1) IN GENERAL.—The Secretary of Defense shall submit to the congressional defense committees a report on the results of the cyber posture review conducted under subsection (a).

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

(3) LIMITATION ON AVAILABILITY OF FUNDS.—Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2018 for operations and maintenance for the Office of the Assistant Secretary of Defense for Public Affairs, not more than 85 percent may be obligated or expended until the date on which the Secretary of Defense submits to the congressional defense committees the report under paragraph (1).

(e) POSTURE REVIEW PERIOD DEFINED.—In this section, the term "posture review period" means the period beginning on the date that is five years after the date of the enactment of this Act and ending on the date that is 10 years after such date of enactment.

SEC. 1645. BRIEFING ON CYBER CAPABILITY AND READINESS SHORTFALLS.

(a) BRIEFING REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary of the Army shall provide to the Committees on Armed Services of Senate and the House of Representatives a briefing on the ability of the Army Combat Training Centers to provide sufficient cyber training for deploying forces.

(b) ELEMENTS.—The briefing under subsection (a) shall include—

(1) an assessment of the pre-rotational training requirements for all deploying Army forces relating to the conduct of, and response to, cyber electromagnetic activities;

(2) an assessment of the training capabilities of the Army Combat Training Centers with respect to cyber electromagnetic activities; and

(3) recommendations for any improvements to training curricula, exercises, or infrastructure capabilities that may be needed to fill gaps in cyber training capabilities as such gaps are identified in the assessments under paragraphs (1) and (2).

(c) ADDITIONAL CONSIDERATIONS.—In preparing the briefing under subsection (a), the Secretary of the Army shall take into account the resources available within a 10-mile radius of the Army Combat Training Centers that could be used to address potential cyber capability and readiness shortfalls, including resources from other military departments, defense agencies, and field activities.

(d) CYBER ELECTROMAGNETIC ACTIVITIES DEFINED.—In this section, the term "cyber electromagnetic activities" has the meaning given the term in the Army Field Manual 3–38 titled "Cyber Electromagnetic Activities".

SEC. 1646. BRIEFING ON CYBER APPLICATIONS OF BLOCKCHAIN TECHNOLOGY.

(a) BRIEFING REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, in consultation with the heads of such other departments and agencies of the Federal Government as the Secretary considers appropriate, shall provide to the appropriate committees of Congress a briefing on the cyber applications of blockchain technology.

(b) ELEMENTS.—The briefing under subsection (a) shall include—

(1) a description of potential offensive and defensive cyber applications of blockchain technology and other distributed database technologies;

(2) an assessment of efforts by foreign powers, extremist organizations, and criminal networks to utilize such technologies;

(3) an assessment of the use or planned use of such technologies by the Federal Government and critical infrastructure networks; and

(4) an assessment of the vulnerabilities of critical infrastructure networks to cyber attacks.

(c) FORM OF BRIEFING.—The briefing under subsection (a) shall be provided in unclassified form, but may include a classified supplement.

(d) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term "appropriate committees of Congress" means—

(1) the Committee on Armed Services, the Select Committee on Intelligence, the Committee on Banking, Housing, and Urban Affairs, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Committee on Armed Services, the Permanent Select Committee on Intelligence, the Committee on Financial Services, and the Committee on Homeland Security of the House of Representatives.

SEC. 1647. BRIEFING ON TRAINING INFRASTRUCTURE FOR CYBER MISSION FORCES.

Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall provide to the congressional defense committees a briefing on the Department of Defense training infrastructure for cyber mission forces. Such briefing shall include the following:

(1) A strategic plan for the growth and expansion of the training infrastructure for cyber mission forces across the Department of Defense commensurate with the projected growth of the cyber mission force.

(2) Identification of the shortcomings in such training infrastructure.

(3) A plan for the management and oversight of such training infrastructure, including management and oversight of the implementation of the strategic plan described in paragraph (1).

(4) Commercial applications that may potentially be used to address the needs identified in the strategic plan described in paragraph (1).

SEC. 1648. REPORT ON TERMINATION OF DUAL-HAT ARRANGEMENT FOR COMMANDER OF THE UNITED STATES CYBER COMMAND.

(a) REPORT.—Not later than May 1, 2018, the Secretary of Defense shall submit to the appropriate congressional committees a report on the progress of the Department of Defense in meeting the requirements of section 1642 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 130 Stat. 2601).

(b) ELEMENTS.—The report under subsection (a) shall include, with respect to any decision to terminate the dual-hat arrangement as described in section 1642 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 130 Stat. 2601), the following:

(1) Metrics and milestones for meeting the conditions described in subsection (b)(2)(C) of such section 1642.

(2) Identification of any challenges to meeting such conditions.

(3) Using data and support from the Director of Cost Assessment and Program Evaluation, in consultation with the Commander of the United States Cyber Command and the Director of the National Security Agency, identification of the costs that may be incurred in the effort to meet such conditions.

(4) Identification of entities or persons requiring additional resources as a result of any decision to terminate the dual-hat arrangement.

(5) Identification of any updates to statutory authorities needed as a result of any decision to terminate the dual-hat arrangement.

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

(1) the congressional defense committees;

(2) the Select Committee on Intelligence of the Senate; and

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

PART II—CYBERSECURITY EDUCATION

SEC. 1649. CYBER SCHOLARSHIP PROGRAM.

(a) NAME OF PROGRAM.—Section 2200 of title 10, Unites States Code, is amended by adding at the end the following:

"(c) NAME OF PROGRAM.—The programs authorized under this chapter shall be known as the 'Cyber Scholarship Program'.".

(b) MODIFICATION TO ALLOCATION OF FUNDING FOR CYBER SCHOLARSHIP PROGRAM.—Section 2200a(f) of title 10, Unites States Code, is amended—

(1) by inserting "(1)" before "Not less"; and

(2) by adding at the end the following new paragraph:

"(2) Not less than five percent of the amount available for financial assistance under this section for a fiscal year shall be available for providing financial assistance for the pursuit of an associate degree at an institution described in paragraph (1).".

(c) CYBER DEFINITION.—Section 2200e of title 10, Unites States Code, is amended to read as follows:

"§ 2200e. Definitions

"In this chapter:

"(1) The term 'cyber' includes the following:

"(A) Offensive cyber operations.

"(B) Defensive cyber operations.

"(C) Department of Defense information network operations and defense.

"(D) Any other information technology that the Secretary of Defense considers to be related to the cyber activities of the Department of Defense.

"(2) The term 'institution of higher education' has the meaning given the term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).

"(3) The term 'Center of Academic Excellence in Cyber Education' means an institution of higher education that is designated by the Director of the National Security Agency as a Center of Academic Excellence in Cyber Education.".

(d) CONFORMING AMENDMENTS.—

(1) Chapter 112 of title 10, United States Code, is further amended—

(A) in the chapter heading, by striking "**INFORMATION SECURITY**" and inserting "**CYBER**";

(B) in section 2200 (as amended by subsection (a))—

(i) in subsection (a), by striking "Department of Defense information assurance requirements" and inserting "the cyber requirements of the Department of Defense"; and

(ii) in subsection (b)(1), by striking "information assurance" and inserting "cyber disciplines";

(C) in section 2200a (as amended by subsection (b))—

(i) in subsection (a)(1), by striking "an information assurance discipline" and inserting "a cyber discipline";

(ii) in subsection (f)(1), by striking "information assurance" and inserting "cyber disciplines"; and

(iii) in subsection (g)(1), by striking "an information technology position" and inserting "a cyber position";

(D) in section 2200b, by striking "information assurance disciplines" and inserting "cyber disciplines";

(E) in the heading of section 2200c, by striking "**Information Assurance**" and inserting "**Cyber**"; and

(F) in section 2200c, by striking "Information Assurance" each place it appears and inserting "Cyber".

(2) The table of sections at the beginning of chapter 112 of title 10, United States Code, is amended by striking the item relating to section 2200c and inserting the following:

"2200c. Centers of Academic Excellence in Cyber Education.".

(3) Section 7045 of title 10, United States Code, is amended—

(A) by striking "Information Security Scholarship program" each place it appears and inserting "Cyber Scholarship program"; and

(B) in subsection (a)(2)(B), by striking "information assurance" and inserting "a cyber discipline".

(4) Section 7904(4) of title 38, United States Code, is amended by striking "Information Assurance" and inserting "Cyber".

(e) REDESIGNATIONS.—

(1) SCHOLARSHIP PROGRAM.—The Information Security Scholarship program under chapter 112 of title 10, United States Code, is redesignated as the "Cyber Scholarship program". Any reference in a law (other than this section), map, regulation, document, paper, or other record of the United States to the Information Security Scholarship program shall be deemed to be a reference to the Cyber Scholarship Program.

(2) CENTERS OF ACADEMIC EXCELLENCE.—Any institution of higher education designated by the Director of the National Security Agency as a Center of Academic Excellence in Information Assurance Education is redesignated as a Center of Academic Excellence in Cyber Education. Any reference in a law (other than this section), map, regulation, document, paper, or other record of the United States to a Center of Academic Excellence in Information Assurance Education shall be deemed to be a reference to a Center of Academic Excellence in Cyber Education.

(f) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Secretary of Defense to provide financial assistance under section 2200a of title 10, United States Code (as amended by this section), and grants under section 2200b of such title (as so amended), $10,000,000 for fiscal year 2018.

SEC. 1649A. COMMUNITY COLLEGE CYBER PILOT PROGRAM AND ASSESSMENT.

(a) PILOT PROGRAM.—Not later than 1 year after the date of enactment of this subtitle, as part of the Federal Cyber Scholarship-for-Service program established under section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442), the Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management, shall develop and implement a pilot program at not more than 10, but at least 5, community colleges to provide scholarships to eligible students who—

(1) are pursuing associate degrees or specialized program certifications in the field of cybersecurity; and

(2)(A) have bachelor's degrees; or

(B) are veterans of the Armed Forces.

(b) ASSESSMENT.—Not later than 1 year after the date of enactment of this subtitle, as part of the Federal Cyber Scholarship-for-Service program established under section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442), the Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management, shall assess the potential benefits and feasibility of providing scholarships through community colleges to eligible students who are pursuing associate degrees, but do not have bachelor's degrees.

SEC. 1649B. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM UPDATES.

(a) IN GENERAL.—Section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442) is amended—

(1) in subsection (b)—

(A) in paragraph (2), by striking "and" at the end; and

(B) by striking paragraph (3) and inserting the following:

"(3) prioritize the employment placement of at least 80 percent of scholarship recipients in an executive agency (as defined in section 105 of title 5, United States Code); and

"(4) provide awards to improve cybersecurity education at the kindergarten through grade 12 level—

"(A) to increase interest in cybersecurity careers;

"(B) to help students practice correct and safe online behavior and understand the foundational principles of cybersecurity;

"(C) to improve teaching methods for delivering cybersecurity content for kindergarten through grade 12 computer science curricula; and

"(D) to promote teacher recruitment in the field of cybersecurity.";

(2) by amending subsection (d) to read as follows:

"(d) POST-AWARD EMPLOYMENT OBLIGATIONS.—Each scholarship recipient, as a condition of receiving a scholarship under the program, shall enter into an agreement under which the recipient agrees to work for a period equal to the length of the scholarship, following receipt of the student's degree, in the cybersecurity mission of—

"(1) an executive agency (as defined in section 105 of title 5, United States Code);

"(2) Congress, including any agency, entity, office, or commission established in the legislative branch;

"(3) an interstate agency;

"(4) a State, local, or Tribal government; or

"(5) a State, local, or Tribal government-affiliated nonprofit that is considered to be critical infrastructure (as defined in section 1016(e) of the USA Patriot Act (42 U.S.C. 5195c(e)).";

(3) in subsection (f)—

(A) by amending paragraph (3) to read as follows:

"(3) have demonstrated a high level of competency in relevant knowledge, skills, and abilities, as defined by the national

cybersecurity awareness and education program under section 401;"; and

(B) by amending paragraph (4) to read as follows:

"(4) be a full-time student in an eligible degree program at a qualified institution of higher education, as determined by the Director of the National Science Foundation, except that in the case of a student who is enrolled in a community college, be a student pursuing a degree on a less than full-time basis, but not less than half-time basis; and"; and

(4) by amending subsection (m) to read as follows:

"(m) PUBLIC INFORMATION.—

"(1) EVALUATION.—The Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management, shall periodically evaluate and make public, in a manner that protects the personally identifiable information of scholarship recipients, information on the success of recruiting individuals for scholarships under this section and on hiring and retaining those individuals in the public sector cyber workforce, including information on—

"(A) placement rates;

"(B) where students are placed, including job titles and descriptions;

"(C) salary ranges for students not released from obligations under this section;

"(D) how long after graduation students are placed;

"(E) how long students stay in the positions they enter upon graduation;

"(F) how many students are released from obligations; and

"(G) what, if any, remedial training is required.

"(2) REPORTS.—The Director of the National Science Foundation, in coordination with the Office of Personnel Management, shall submit, not less frequently than once every 3 years, to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives a report, including the results of the evaluation under paragraph (1) and any recent statistics regarding the size, composition, and educational requirements of the Federal cyber workforce.

"(3) RESOURCES.—The Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management, shall provide consolidated and user-friendly online resources for prospective scholarship recipients, including, to the extent practicable—

"(A) searchable, up-to-date, and accurate information about participating institutions of higher education and job opportunities related to the field of cybersecurity; and

"(B) a modernized description of cybersecurity careers.".

(b) SAVINGS PROVISION.—Nothing in this section, or an amendment made by this section, shall affect any agreement, scholarship, loan, or repayment, under section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442), in effect on the day before the date of enactment of this subtitle.

SEC. 1649C. CYBERSECURITY TEACHING.

Section 10(i) of the National Science Foundation Authorization Act of 2002 (42 U.S.C. 1862n–1(i)) is amended—

(1) by amending paragraph (5) to read as follows:

"(5) the term 'mathematics and science teacher' means a science, technology, engineering, mathematics, or computer science, including cybersecurity, teacher at the elementary school or secondary school level;"; and

(2) by amending paragraph (7) to read as follows:

"(7) the term 'science, technology, engineering, or mathematics professional' means an individual who holds a baccalaureate, master's, or doctoral degree in science, technology, engineering, mathematics, or computer science, including cybersecurity, and is working in or had a career in such field or a related area; and".

Subtitle D—Nuclear Forces

SEC. 1651. ANNUAL ASSESSMENT OF CYBER RESILIENCY OF NUCLEAR COMMAND AND CONTROL SYSTEM.

(a) IN GENERAL.—Chapter 24 of title 10, United States Code, is amended by adding at the end the following new section:

"§ 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) REPORT REQUIRED.—(1) 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 required by subsection (a) 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.