Subtitle C—Cyber Warfare, Cybersecurity, and Related Matters

SEC. 1621. POLICY OF THE UNITED STATES ON CYBERSPACE, CYBERSECURITY, AND CYBER WARFARE.

(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 when necessary, to any and all cyber attacks or other malicious cyber activities that target United States interests with the intent to—

(1) cause casualties among United States persons or persons of our 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 United States Armed Forces, the freedom of maneuver of the United States 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 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 demonstrate, or otherwise make known to adversaries of 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—

(1) devote immediate and sustained attention to 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;

(2) develop 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;

(3) enhance attribution capabilities to reduce the time required to positively attribute an attack with high confidence; and

(4) develop intelligence and offensive cyber capabilities to detect, disrupt, and potentially expose malicious cyber activities.

(f) POLICIES RELATING TO OFFENSIVE CYBER CAPABILITIES AND SOVEREIGNTY.—It is the policy of the United

States that, when a cyber attack or malicious cyber activity transits or otherwise relies upon the networks or infrastructure of a third country—

(1) the United States shall, to the greatest extent practicable, notify and encourage the government of that country to take action to eliminate the threat; and

(2) if the government is unable or unwilling to take action, the United States reserves the right to act unilaterally (with the consent of that government if possible, but without such consent if necessary).

(g) AUTHORITY OF SECRETARY OF DEFENSE.—

(1) IN GENERAL.—The Secretary of Defense has the authority to develop, prepare, coordinate, and, when appropriately authorized to do so, conduct military cyber operations in response to cyber attacks and malicious cyber activities described in subsection (a) that are carried out against the United States or United States persons by a foreign power.

(2) DELEGATION OF ADDITIONAL AUTHORITIES.—The Secretary may delegate to the Commander of the United States Cyber Command such authorities of the Secretaries of the military departments, including authorities relating to manning, training, and equipping, that the Secretary considers appropriate.

(3) USE OF DELEGATED AUTHORITIES.—The use by the Commander of the United States Cyber Command of any authority delegated to the Commander pursuant to this subsection shall be subject to the authority, direction, and control of the Secretary.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit the authority of the President or Congress to authorize the use of military force.

(h) FOREIGN POWER DEFINED.—In this section, 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).

SEC. 1622. CYBER POSTURE REVIEW.

(a) REQUIREMENT FOR COMPREHENSIVE REVIEW.—In order to clarify United States cyber deterrence policy and strategy for the near term, the Secretary of Defense shall conduct a comprehensive review of the cyber posture of the United States for the next 5 to 10 years. The Secretary shall conduct the review in consultation with the Director of National Intelligence, the Attorney General, the Secretary of the Department of Homeland Security, and the Secretary of State.

(b) ELEMENTS OF REVIEW.—The cyber posture review shall include the following elements:

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

(2) A declaratory policy relating to United States responses to cyber attack and use of offensive cyber capabilities, guidance for the employment of offensive cyber capabilities, a public affairs plan, and an engagement plan for adversaries and allies.

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

(4) Guidance for the development of cyber deterrence campaign plans focused on key leadership of Russia, China, Iran, North Korea, and any other country the Secretary determines appropriate.

(5) Examination through analysis and gaming of escalation dynamics in various scenarios, as well as the spiral escalatory effects of countries developing increasingly potent offensive cyber capabilities, and what steps should be undertaken to bolster stability in cyberspace and more broadly stability between major powers.

(6) A certification of whether sufficient personnel are trained and equipped to meet validated cyber requirements.

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

(c) REPORT TO CONGRESS.—Not later than March 1, 2018, the Secretary of Defense shall submit to Congress, in unclassified and classified forms as necessary, a report on the results of the cyber posture review conducted under this section.

(d) SENSE OF CONGRESS.—It is the sense of Congress that the United States should respond to all cyber attacks and to all significant cyber intrusions by imposing costs on those responsible that exceed any benefit that the attacker or intruder may have hoped to gain.

SEC. 1623. MODIFICATION AND CLARIFICATION OF REQUIREMENTS AND AUTHORITIES RELATING TO ESTABLISHMENT OF UNIFIED COMBATANT COMMAND FOR CYBER OPERATIONS.

(a) DEADLINE FOR ESTABLISHMENT.—Before the Cyber Mission Force reaches full operational capability, the President shall establish the unified combatant command for cyber operations forces pursuant to section 167b(a) of title 10, United State Code.

(b) CLARIFICATION OF FUNCTIONS.—Subsection (a) of section 167b of title 10, United States Code, is amended—

(1) by striking the second sentence;

(2) by inserting "(1)" before "With the"; and

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

"(2) The principal functions of the cyber command are as follows:

"(A) To execute cyber operations.

"(B) To prepare cyber operations forces to carry out assigned missions.".

(c) MODIFICATION OF ASSIGNMENT OF FORCES.—Subsection (b) of such section is amended by striking "stationed in the United States".

(d) MODIFICATION OF COMMAND OF ACTIVITY OR MISSION.—Subsection (d) of such section is amended to read as follows:

"(d) COMMAND OF ACTIVITY OR MISSION.—The commander of the cyber command shall execute and exercise command of cyberspace operations and coordinate with the affected commanders of the unified combatant commands, unless otherwise directed by the President or the Secretary of Defense.".

(e) MODIFICATION OF AUTHORITY OF COMBATANT COMMANDER.—Subsection (e)(2)(A) of such section is amended—

(1) in clause (iii)—

(A) in subclause (I), by striking "and" at the end;

(B) in subclause (II), by striking "assigned to unified combatant commands";

(C) by redesignating subclause (II) as subclause (III); and

(D) by inserting after subclause (I) the following new subclause (II):

"(II) for development and acquisition of joint cyber capabilities; and";

(2) in clause (iv), by striking "joint" and inserting "cyber operations"; and

(3) in clause (v), by striking "commissioned and noncommissioned officers" and inserting "cyber operations forces".

SEC. 1624. 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 (in this section referred to as the 'Council'), 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.

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

"(3) The Secretary of Defense shall submit to the congressional defense committees the report required by paragraph (1), any comments of the Council on the report under paragraph (2), and any comments of the Secretary on the report.

"(d) TERMINATION.—This section shall terminate on the date that is 10 years after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2018.".

(b) CLERICAL AMENDMENT.—The table of sections for chapter 24 of such title is amended by inserting after the item relating to section 498 the following new item:

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

SEC. 1625. STRATEGIC CYBERSECURITY PROGRAM.

(a) IN GENERAL.—The Secretary of Defense shall establish 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 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 responsibility to be discharged by the Program. 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) RESPONSIBILITY.—

(1) IN GENERAL.—The responsibility of the Program shall be to carry out activities (commonly referred to as "red-teaming") to continuously assess the information assurance and improve the overall effectiveness of the following of the United States 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 Author-

ization Act for Fiscal Year 2017 (Public Law 114–329)).

(2) SCOPE OF RESPONSIBILITY.—In carrying out its activities, the Program shall carry out appropriate reviews of current 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 by the Program pursuant to paragraph (2), including any remedial action recommended by the Program 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) REPORTS.—The Director of the National Security Agency shall submit to the Secretary of Defense and the congressional defense committees on a quarterly basis a report on the activities of the Program during the preceding calendar quarter. Each report shall include the following:

(1) A description of the activities of the Program during the calendar quarter covered by such report.

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

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

(e) FUNDING.—Of the amount authorized to be appropriated for fiscal year 2018 for operation and maintenance, Defense-wide, by section 301 and available for the Information Systems Security Program as specified in the funding table in section 4301, up to $100,000,000 may be available for the Strategic Cybersecurity Program and its activities in fiscal year 2018.

(f) SENSE OF CONGRESS.—It is the sense of Congress that the activities conducted under the Program should address the most critical systems of the Department of Defense and should supplement, not supplant, the Cyber Protection Teams of the Department of Defense.

SEC. 1626. EVALUATION OF AGILE ACQUISITION OF CYBER TOOLS AND APPLICATIONS.

(a) EVALUATION REQUIRED.—The Commander of the United States Cyber Command 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 Forces Cyber Command, and the Marine Corps Cyberspace Command.

(b) GOAL.—The goal of the evaluation required by subsection (a) is 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 cyber tools and applications; and

(3) create a repeatable, disciplined process for developing, acquiring, and maintaining cyber tools and applications whereby progress and success or failure can be continuously measured.

(c) CONSIDERATION OF AGILE SOFTWARE DEVELOPMENT, AGILE ACQUISITION, AND OTHER BEST PRACTICES.—

(1) IN GENERAL.—The evaluation required by subsection (a) shall include consideration of agile software development, agile acquisition, and such 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), consider changes

that would be necessary to established acquisition practices, including 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 conducting 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 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, including all aspects of implementation necessary for the success of the recommended methods.

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

(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 exercising of the acquisition authority of the Commander of United States

Cyber Command under section 807 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 10 U.S.C. 2224 note).

(h) DEFINITIONS.—In this section:

(1) The term "agile acquisition" means acquisition pursuant to a methodology for delivering multiple, rapid, incremental capabilities to the user for operational use, evaluation, and feedback. The incremental development and fielding of capabilities, commonly called "spirals", "spins", or "sprints", can be measured in a few weeks or months, and involve continuous participation and collaboration by users, testers, and requirements authorities.

(2) The term "agile development" means development pursuant to a set of software development methodologies based on iterative development, in which requirements and solutions evolve through collaboration between self-organizing cross-functional teams.

SEC. 1627. REPORT ON COST IMPLICATIONS OF TERMINATING DUAL-HAT ARRANGEMENT FOR COMMANDER OF UNITED STATES CYBER COMMAND.

Not later than 90 days after the date of the enactment of this Act, the Commander of the United States Cyber Command shall submit to the congressional defense commit-

tees a report that identifies the costs that would be implicated by meeting the conditions set forth in section 1642(b)(2)(C) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328).

SEC. 1628. MODIFICATION OF INFORMATION ASSURANCE SCHOLARSHIP PROGRAM.

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

"(h) DESIGNATION OF PROGRAM.—A program under which the Secretary provides financial assistance under subsection (a) shall be known as the 'Department of Defense Cybersecurity Scholarship Program'.".

(b) ALLOCATION OF FUNDING.—Subsection (f) of such section 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.".

(c) REINVIGORATION PLAN REQUIRED.—Not later than September 30, 2018, the Secretary of Defense shall submit to the congressional defense committees a plan for rein-

vigorating the Department of Defense Cyber Scholarship Program authorized under section 2200a of such title, as amended by subsections (a) and (b).

SEC. 1629. MEASURING COMPLIANCE OF COMPONENTS OF DEPARTMENT OF DEFENSE WITH CYBERSECURITY REQUIREMENTS FOR SECURING INDUSTRIAL CONTROL SYSTEMS.

(a) IN GENERAL.—The Secretary of Defense shall make such changes to the scorecard as are necessary to ensure that the Secretary measures each component of the Department of Defense in its progress towards securing the industrial control systems of the Department against cyber threats, including supervisory control and data acquisition systems (SCADA), distributed control systems (DCS), programmable logic controllers (PLC), and platform information technology (PIT).

(b) SCORECARD DEFINED.—In this section, the term "scorecard" means the Department of Defense Cyber Scorecard for the measuring of the performance of components of the Department against basic cybersecurity requirements as outlined in the Department of Defense Cybersecurity Discipline Implementation Plan.

SEC. 1630. EXERCISE ON ASSESSING CYBERSECURITY SUPPORT TO ELECTION SYSTEMS OF STATES.

(a) INCLUSION OF CYBER VULNERABILITIES IN ELECTION SYSTEMS IN CYBER GUARD EXERCISES.—The Secretary of Defense shall incorporate the cybersecurity of elections systems of the States as a component of the Cyber Guard Exercise.

(b) REPORT ON BEST PRACTICES.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report on the capabilities, readiness, and best practices of the National Guard to assist the Governors, if called upon, to defend elections systems from cyberattacks.

SEC. 1630A. REPORT ON VARIOUS APPROACHES TO CYBER DETERRENCE.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report on various approaches to cyber deterrence.

(b) CONTENTS.—The report required by subsection (a) shall include the following:

(1) Identification, definition, and explanation of the various theoretical approaches to cyber deterrence.

(2) An assessment of the relative strengths and weaknesses of each of such approaches relative to the threat and relative to one another.

(3) A recommendation for a cyber deterrence theory and doctrine for the Armed Forces.

(4) An alternative analysis or dissenting view of the recommendation included under paragraph (3) that explains the weaknesses of the recommended theory and doctrine and offers an alternative theory or doctrine.

(c) CONSULTATION.—In preparing the report required by subsection (a), the Secretary shall consult with experts from the Government, industry, and academia.

SEC. 1630B. PROHIBITION ON USE OF SOFTWARE PLATFORMS DEVELOPED BY KASPERSKY LAB.

(a) PROHIBITION.—No department, agency, organization, or other element of the Department of Defense may use, whether directly or through work with or on behalf of another organization or element of the Department or another department or agency of the United States Government, any software platform developed, in whole or in part, by Kaspersky Lab or any entity of which Kaspersky Lab has a majority ownership.

(b) SEVERANCE OF NETWORK CONNECTIONS.—The Secretary of Defense shall ensure that any network connection between a department, agency, organization, or other element of the Department of Defense and a department or agency of the United States Government that is using or

hosting on its networks a software platform described in subsection (a) is immediately severed.

(c) EFFECTIVE DATE.—This section shall take effect on October 1, 2018.

SEC. 1630C. REPORT ON CYBER APPLICATIONS OF BLOCKCHAIN TECHNOLOGY.

(a) REPORT 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 agencies and departments as the Secretary considers appropriate, shall submit to the appropriate committees of Congress a report on the potential offensive and defensive cyber applications of blockchain technology and other distributed database technologies and an assessment of efforts by foreign powers, extremist organizations, and criminal networks to utilize these technologies. Such report shall also include an assessment of the use or planned use of blockchain technologies by the United States Government or critical infrastructure networks and the vulnerabilities of such networks to cyber attacks.

(b) FORM OF REPORT.—The report required by (a) may be submitted—

(1) in classified form; or

(2) in unclassified form with a classified annex.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu