# H.R. 5515—FY19 NATIONAL DEFENSE AUTHORIZATION BILL

# SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

# SUMMARY OF BILL LANGUAGE

# Table Of Contents

# DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

## TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

### LEGISLATIVE PROVISIONS

#### SUBTITLE B—PROGRAM REQUIREMENTS, RESTRICTIONS, AND LIMITATIONS

##### Section 211—Modification of Authority to Carry Out Certain Prototype Projects

This section would make modifications to section 2371b of title 10, United States Code, regarding use of transactions other than contracts and grants for follow-on production.

##### Section 212—Extension of Directed Energy Prototyping Authority

This section would extend the directed energy prototype authority provided for in section 219(c)(4) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328) through fiscal year 2019.

##### Section 217—Limitation on Availability of Funds for Certain High Energy Laser Advanced Technology

This section would limit the availability of 50 percent of the funds authorized to be appropriated by this Act, or otherwise made available for fiscal year 2019, until the Secretary of Defense provides the High Energy Laser logical roadmap and assessment to the congressional defense committees.

##### Section 218—Plan for Elimination or Transfer of the Strategic Capabilities Office of the Department of Defense

This section would direct the Secretary of Defense to submit a plan to the congressional defense committees by March 1, 2019, for the elimination or transfer of the functions of the Strategic Capabilities Office to another organization or element of the Department of Defense.

#### SUBTITLE C—REPORTS AND OTHER MATTERS

##### Section 224—Briefing on Use of Quantum Sciences for Military Applications and Other Purposes

This section would require the Secretary of Defense to provide to the congressional defense committees a briefing and plan for using quantum sciences for military applications and other purposes.

# TITLE V—MILITARY PERSONNEL POLICY

## LEGISLATIVE PROVISIONS

### SUBTITLE E—DEFENSE DEPENDENTS' EDUCATION AND MILITARY FAMILY READINESS MATTERS

#### Section 541—Enhancement and Clarification of Family Support Services for Family Members of Members of Special Operations Forces

This section would amend section 1788a of title 10, United States Code, to provide greater flexibility to support the family requirements to tactical units by increasing funds available for Major Force Program 11 from $5.0 million to $10.0 million. This section would also define the term "family support services" to provide clarity and authorize proper expenditures of appropriated funds.

# TITLE VIII—ACQUISITION POLICY, ACQUISITION MANAGEMENT, AND RELATED MATTERS

## LEGISLATIVE PROVISIONS

### SUBTITLE E—SMALL BUSINESS MATTERS

#### Section 855—Consolidated Budget Justification for the Department of Defense Small Business Innovation Research Program and Small Business Technology Transfer Program

This section would direct the Secretary of Defense to submit to Congress a budget justification for all activities conducted under the Small Business Innovation Research Program or Small Business Technology Transfer Program during the previous fiscal year.

# TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

## LEGISLATIVE PROVISIONS

### SUBTITLE C—OTHER MATTERS

#### Section 921—Artificial Intelligence and Machine Learning Policy and Oversight Council

This section would direct the Under Secretary of Research and Engineering to establish an Artificial Intelligence and Machine Learning Policy and Oversight

Council to continuously improve research, innovation, policy, joint processes, and procedures that facilitate the development, acquisition, integration, advancement, and sustainment of artificial intelligence and machine learning throughout the Department of Defense.

# TITLE X—GENERAL PROVISIONS

## LEGISLATIVE PROVISIONS

### SUBTITLE D—COUNTERTERRORISM

#### Section 1031—Definition of Sensitive Military Operation

This section would modify section 130f of title 10, United States Code, regarding notification requirements for sensitive military operations.

### SUBTITLE F—STUDIES AND REPORTS

#### Section 1051—Department of Defense Review and Assessment on Advances in Artificial Intelligence and Machine Learning

This section would direct the Secretary of Defense, acting through the Defense Innovation Board and the Under Secretary of Defense for Research and Engineering, to carry out a review and assessment of the advances in artificial intelligence, related machine learning developments, and associated technologies for military applications. This section would also require the Secretary of Defense to submit an initial report to the congressional defense committees not later than 180 days after the date of the enactment of this Act, and a comprehensive report not later than 1 year after the date of the enactment of this Act.

#### Section 1053—Report on Proposed Consolidation of Department of Defense Global Messaging and Counter Messaging Capabilities

This section would limit the availability of funds authorized to be appropriated by this Act, or otherwise made available for fiscal year 2019, until the Secretary of Defense provides a report to the congressional defense committees on the Department of Defense Global Messaging and Counter Messaging program.

#### Section 1054—Comprehensive Review of Professionalism and Ethics Programs for Special Operations Forces

This section would direct the Secretary of Defense, in coordination with the Secretaries of the military departments, to conduct a comprehensive review of the ethics and professionalism programs of the U.S. Special Operations Command and the military departments for officers and other military personnel serving in special

operations forces. This section would require the Secretary of Defense to submit the review to the Committees on Armed Services of the Senate and the House of Representatives by March 1, 2019.

### SUBTITLE G—OTHER MATTERS

#### Section 1062—Principal Advisor on Countering Weapons of Mass Destruction

This section would direct the Secretary of Defense to designate, from among the personnel of the Office of the Secretary of Defense, a Principal Advisor on Countering Weapons of Mass Destruction (CWMD). Such individual shall act as the Principal Advisor to the Secretary on the activities of the Department of Defense relating to countering weapons of mass destruction. Further, this section would require a plan for realigning, restructuring, or reducing the current CWMD oversight framework of the Office of the Secretary of Defense.

## TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

### LEGISLATIVE PROVISIONS

### SUBTITLE A—ASSISTANCE AND TRAINING

#### Section 1203—NATO Strategic Communications Center of Excellence

This section would authorize the Secretary of Defense to provide funds for fiscal year 2019 for the purposes of supporting the NATO Strategic Communications Center of Excellence, and would direct the Secretary of Defense to assign executive agent responsibilities to an appropriate organization within the Department of Defense.

#### Section 1204—NATO Cooperative Cyber Defense Center of Excellence

This section would authorize the Secretary of Defense to provide funds for fiscal year 2019 for the purposes of supporting the NATO Cooperative Cyber Defense Center of Excellence, and would direct the Secretary of Defense to assign executive agent responsibilities to an appropriate organization within the Department of Defense.

### SUBTITLE F—OTHER MATTERS

#### Section 1256—United States-Israel Countering Unmanned Aerial Systems Cooperation

This section would modify section 1279 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92) to authorize

establishment of a cooperative research and development program with the State of Israel to develop capabilities for countering unmanned aerial systems through modification of the existing memorandum of agreement between the United States and Israel for anti-tunneling defense capabilities or through a new memorandum of agreement.

### Section 1257—Three-Year Extension of Authorization of Non-Conventional Assisted Recovery Capabilities

This section would modify section 943(g) of the National Defense Authorization Act for Fiscal Year 2009 (Public Law 110–417), as most recently amended by section 1051(n) of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115-91), authorization of non-conventional assisted recovery capabilities, by striking "2021" and inserting "2024".

## TITLE XIII—COOPERATIVE THREAT REDUCTION

### LEGISLATIVE PROVISIONS

### Section 1301—Funding Allocations

This section would allocate specific funding amounts for each program under the Department of Defense Cooperative Threat Reduction (CTR) Program from within the overall $335.2 million that the committee would authorize for the CTR Program. The allocation under this section reflects the amount of the budget request for fiscal year 2019.

### Section 1302—Specification of Cooperative Threat Reduction Funds

This section would specify that funds authorized to be appropriated to the Department of Defense for the Cooperative Threat Reduction Program, established under the Department of Defense Cooperative Threat Reduction Act (50 U.S.C. 3711), would be available for obligation in fiscal years 2019, 2020, and 2021.

## TITLE XIV—OTHER AUTHORIZATIONS

### LEGISLATIVE PROVISIONS

### SUBTITLE B—OTHER MATTERS

### Section 1413—Quarterly Briefing on Progress of Chemical Demilitarization Program

This section would modify section 1521 of title 50, United States Code, to require the Secretary of Defense to provide quarterly briefings to the congressional defense committees on the progress of the chemical demilitarization program, including contractor cost and schedule performance, destruction progress, and any other relevant information until stockpile destruction is complete. This section would also eliminate the semiannual written reports required in the section referenced above.

## TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

## LEGISLATIVE PROVISIONS

### SUBTITLE C—CYBERSPACE-RELATED MATTERS

### Section 1631—Amendments to Pilot Program Regarding Cyber Vulnerabilities of Department of Defense Critical Infrastructure

This section would modify subsection (b) of section 1650 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328) to incorporate the Defense Digital Service (DDS) into pilot program authorities for identifying new, innovative methodologies or engineering approaches to evaluate cyber vulnerabilities of Department of Defense critical infrastructure. The committee notes the success of the Defense Digital Service's "Hack the Pentagon" program, and encourages the Department to use this or similar DDS activities to more rapidly and effectively improve the cybersecurity of government owned and operated facilities.

### Section 1632—Budget Display for Cyber Vulnerability Evaluations and Mitigation Activities for Major Weapon Systems of the Department of Defense

This section would require that the justification materials submitted to Congress by the Secretary of Defense in support of the President's annual budget request for the Department of Defense include a consolidated display for cyber vulnerability evaluations and mitigation activities for each major weapon system beginning in fiscal year 2021. The display for each major weapon system shall include the status of, funding required, and a description of planned activities to continue or complete the cyber vulnerability evaluations in accordance with section 1647 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92), and necessary mitigation activities for the Future Years Defense Program.

Section 1633—Transfer of Responsibility for the Department of Defense Information Network to United States Cyber Command

This section would mandate that the Secretary of Defense transfer of all roles, missions, and responsibilities of the Commander, Joint Force Headquarters-Department of Defense Information Networks from the Defense Information Support Agency to Commander, United States Cyber Command, by September 30, 2019. It would additionally require the Secretary of Defense to certify in writing to the congressional defense committees that such transfer shall not result in mission degradation.

Section 1634—Pilot Program Authority to Enhance Cybersecurity and Resiliency of Critical Infrastructure

This section would authorize the Secretary of Defense, in coordination with the Secretary of Homeland Security, to provide technical personnel to the Department of Homeland Security to enhance cooperation, collaboration, and unity of government efforts in support of the protection of critical infrastructure from cyber incidents and significant cyber incidents.

Section 1635—Procedures and Reporting Requirement on Cybersecurity Breaches and Loss of Personally Identifiable Information

This section would require the Secretary of Defense to promptly notify the congressional defense committees in the event of a significant loss of personally identifiable information of civilian or uniformed members of the Armed Forces in classified or unclassified formats.

Section 1636—Study and Report on Reserve Component Cyber Civil Support Teams

This section would require the Secretary of Defense and the Secretary of Homeland Security to conduct a study on the feasibility and advisability of establishing cyber civil support teams comprised of Reserve Component members, primarily operating under the command and control of the Governor of each State, to prepare for and respond to cyber incidents, cyber emergencies, and cyber attacks. The Secretaries concerned shall provide a report to the congressional defense committees, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate not later than 180 days after the date of the enactment of this Act on the results of the study, to include their final determination on the feasibility of, advisability and necessity of establishing Reserve Component cyber civil support teams for each State, and if so, proposed legislation.

# BILL LANGUAGE

# Subtitle B—Program Requirements, Restrictions, and Limitations

**SEC. 211 [Log 67407]. MODIFICATION OF AUTHORITY TO CARRY OUT CERTAIN PROTOTYPE PROJECTS.**

Section 2371b(f) of title 10, United States Code, is amended by adding at the end the following new paragraphs:

''(4) Contracts or transactions entered into pursuant to this subsection that are expected to cost the Department of Defense in excess of $100,000,000 but not in excess of $500,000,000 (including all options) may be awarded only upon written determination by the senior procurement executive for the agency as designated for the purpose of section 1702(c) of title 41, or, by the senior procurement executive for the Defense Advanced Research Projects Agency or the Missile Defense Agency that award of the contract or transaction is essential to meet critical national security interests.

''(5) Contracts and transactions entered into pursuant to this subsection that are expected to cost the Department of Defense in excess of $500,000,000 (including all options) may be awarded only if—

''(A) the Under Secretary of Defense for Acquisition and Sustainment determines in writing that

award of the contract or transaction is essential to meet critical national security objectives; and

''(B) the congressional defense committees are notified in writing not later than 30 days before award of the contract or transaction.''.

**SEC. 212 [Log 67406]. EXTENSION OF DIRECTED ENERGY PROTOTYPE AUTHORITY.**

Section 219(c)(4) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 10 U.S.C. 2431 note) is amended—

(1) in subparagraph (A), by striking ''Except as provided in subparagraph (B)'' and inserting ''Except as provided in subparagraph (C)'';

(2) by redesignating subparagraph (B) as subparagraph (C);

(3) by inserting after subparagraph (A) the following:

''(B) Except as provided in subparagraph (C) and subject to the availability of appropriations for such purpose, of the funds authorized to be appropriated by the National Defense Authorization Act for Fiscal Year 2019 or otherwise made available for fiscal year 2019 for research, development, test, and evaluation, defense-wide, up to $100,000,000 may be available to the Under Secretary to allocate to the military departments, the defense agencies, and the combatant commands to carry out the program established under paragraph (1).''; and

(4) in subparagraph (C), as so redesignated, by striking ''made available under subparagraph (A)''

and inserting ''made available under subparagraph (A) or subparagraph (B)''.

**SEC. 217 [Log 67739]. LIMITATION ON AVAILABILITY OF FUNDS FOR CERTAIN HIGH ENERGY LASER ADVANCED TECHNOLOGY.**

(a) LIMITATION.—Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2019 for the Department of Defense for High Energy Laser Advanced Technology (PE 0603924D8Z), not more than 50 percent may be obligated or expended until the date on which the Secretary of Defense submits to the congressional defense committees—

(1) a logical roadmap and detailed assessment of the high energy laser programs of the Department of Defense; and

(2) a justification for the $33,533,000 of increased funding for high energy laser programs authorized in the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91).

(b) RULE OF CONSTRUCTION.—The limitation in subsection (a) shall not be construed to apply to any other high energy laser program of the Department of Defense other than the program element specified in such subsection.

**SEC. 218 [Log 67335]. PLAN FOR ELIMINATION OR TRANSFER OF THE STRATEGIC CAPABILITIES OFFICE OF THE DEPARTMENT OF DEFENSE.**

(a) PLAN REQUIRED.—Not later than March 1, 2019, the Secretary of Defense, acting through the Under Secretary of Defense for Research and Engineering, shall submit to the congressional defense committees a plan—

(1) to eliminate the Strategic Capabilities Office of the Department of Defense by not later than October 1, 2020; or

(2) to transfer the functions of the Strategic Capabilities Office to another organization or element of the Department by not later than October 1, 2020.

(b) ELEMENTS.—The plan required under subsection (a) shall include the following:

(1) A timeline for the potential elimination or transfer of the activities, functions, programs, plans, and resources of the Strategic Capabilities Office.

(2) A strategy for mitigating risk to the programs of the Strategic Capabilities Office while the elimination or transfer is carried out.

(3) A strategy for implementing the lessons learned and best practices of the Strategic Capabilities Office across the organizations and elements of

the Department of Defense to promote enterprise-wide innovation.

(c) FORM OF PLAN.—The plan required under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

**SEC. 224 [Log 67300]. BRIEFING ON USE OF QUANTUM SCIENCES FOR MILITARY APPLICATIONS AND OTHER PURPOSES.**

(a) BRIEFING REQUIRED.—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 strategy of the Secretary for using quantum sciences for military applications and other purposes.

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

(1) a description of the knowledge-base of the Department of Defense with respect to quantum sciences and any plans of the Secretary of Defense to enhance such knowledge-base;

(2) a plan that describes how the Secretary intends to use quantum sciences for military applications and to meet other needs of the Department; and

(3) an assessment of the efforts of foreign powers to use quantum sciences for military applications and other purposes.

(c) FORM OF BRIEFING.—The briefing under subsection (a) may be provided in classified or unclassified form.

# Subtitle E—Defense Dependents' Education and Military Family Readiness Matters

**SEC. 541 [log 67363]. ENHANCEMENT AND CLARIFICATION OF FAMILY SUPPORT SERVICES FOR FAMILY MEMBERS OF MEMBERS OF SPECIAL OPERATIONS FORCES.**

Section 1788a of title 10, United States Code, is amended—

(1) by striking ''activities'' each place it appears and inserting ''services'';

(2) in subsection (b)(2), by striking ''activity'' and inserting ''service'';

(3) in subsection (c), by striking ''$5,000,000'' and inserting ''$10,000,000'';

(4) in subsection (d)(1), by striking ''thereafter'' and inserting ''of the next two years''; and

(5) in subsection (e), by adding at the end the following new paragraph:

''(4) The term 'family support services' includes costs of transportation, food, lodging, child care, supplies, fees, and training materials for immediate family members of members of the armed forces assigned to special operations forces while participating in programs under subsection (a).''.

**SEC. 855 [Log 67336]. CONSOLIDATED BUDGET JUSTIFICATION FOR THE DEPARTMENT OF DEFENSE SMALL BUSINESS INNOVATION RESEARCH PROGRAM AND SMALL BUSINESS TECHNOLOGY TRANSFER PROGRAM.**

(a) SUBMISSION WITH ANNUAL BUDGET JUSTIFICATION DOCUMENTS.—The Secretary of Defense, acting through the Under Secretary of Defense for Research and Engineering, shall include in the materials submitted to Congress by the Secretary of Defense in support of the budget of the President for each fiscal year (as submitted to Congress under section 1105 of title 31, United States Code) a budget justification for all activities conducted under a Small Business Innovation Research Program or Small Business Technology Transfer Program (as such terms are defined, respectively, in section 9(e) of the Small Business Act (15 U.S.C. 638(e))) of the Department of Defense during the previous fiscal year.

(b) REQUIREMENTS FOR BUDGET DISPLAY.—The budget justification under subsection (a) shall include—

(1) the amount obligated or expended, by appropriation and functional area, for each activity conducted under a Small Business Innovation Research Program or Small Business Technology Transfer Program, with supporting narrative descriptions and rationale for the funding levels; and

(2) a summary and estimate of funding required during the period covered by the current future-years defense program (as defined under section 221 of title 10, United States Code).

(c) TERMINATION.—The requirements of this section shall terminate on December 31, 2022.

# Subtitle C—Other Matters

**SEC. 921 [Log 67294]. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING POLICY AND OVERSIGHT COUNCIL.**

(a) ESTABLISHMENT.—In order to fulfill the responsibilities specified in Section 133a of title 10, United States Code, the Under Secretary of Defense for Research and Engineering shall establish and lead a team to be known as the ''Artificial Intelligence and Machine Learning Policy and Oversight Council'' (in this section referred to as the ''Council'').

(b) PURPOSE.—The purpose of the Council shall be to—

(1) integrate the functional activities of the organizations and elements of the Department of Defense with respect to artificial intelligence and machine learning;

(2) ensure there are efficient and effective artificial intelligence and machine learning capabilities throughout Department; and

(3) develop and continuously improve research, innovation, policy, joint processes, and procedures to facilitate the development, acquisition, integration, advancement, and sustainment of artificial intel-

ligence and machine learning throughout the Department.

(c) MEMBERSHIP.—The membership of the Council shall include the following:

(1) The Under Secretary of Defense for Research and Engineering, or the designee of the Under Secretary, who shall serve as the leader of the Council.

(2) The following officials of the Department of Defense, or their designees:

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

(B) The Chief Management Officer of the Department of Defense.

(C) The Under Secretary of Defense (Comptroller).

(D) The Under Secretary of Defense for Personnel and Readiness.

(E) The Under Secretary of Defense for Intelligence.

(F) The General Counsel of the Department of Defense.

(G) The head of each military service.

(H) The Commander of the United States Special Operations Command.

(I) The Director of the Defense Advanced Research Projects Agency.

(3) Any other official of the Department of Defense determined to be appropriate by the Under Secretary of Defense for Research and Engineering.

(d) OPERATION.—The Council shall operate continuously.

# Subtitle D—Counterterrorism

**SEC. 1031 [Log 67283]. DEFINITION OF SENSITIVE MILITARY OPERATION.**

Subsection (d) of section 130f of title 10, United States Code, is amended to read as follows:

''(d) SENSITIVE MILITARY OPERATION DEFINED.—(1) Except as provided in paragraph (2), in this section, the term 'sensitive military operation' means a lethal operation or capture operation conducted by the armed forces or conducted by a foreign partner in coordination with the armed forces that targets a specific individual or individuals.

''(2) For purposes of this section, the term 'sensitive military operation' does not include any operation conducted within Afghanistan.''.

# Subtitle F—Studies and Reports

**SEC. 1051 [Log 67295]. DEPARTMENT OF DEFENSE REVIEW AND ASSESSMENT ON ADVANCES IN ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING.**

(a) REVIEW REQUIRED.—The Secretary of Defense, acting through the Defense Innovation Board and the Under Secretary of Defense for Research and Engineering, shall carry out a review and assessment of the advances in artificial intelligence, related machine learning developments, and associated technologies for military applications. In carrying out such review, the Secretary shall consider the methods and means necessary to advance the development of artificial intelligence, machine learning, and associated technologies within the Department of Defense to comprehensively address the national security needs and requirements of the Department of Defense.

(b) SCOPE OF REVIEW.—In conducting the review under paragraph (a) the Secretary of Defense shall consider—

(1) the competitiveness of the Department of Defense in artificial intelligence, machine learning, and other associated technologies, including matters pertaining to public-private partnerships and investments;

(2) means and methods for the Department of Defense to maintain a technological advantage in artificial intelligence, machine learning, and other associated technologies, including quantum sciences and high performance computing;

(3) means by which the Department of Defense can help foster greater emphasis and investments in basic and advanced research to stimulate private, public, academic, and combined initiatives in artificial intelligence, machine learning, and other associated technologies, including quantum sciences, and high performance computing;

(4) Department of Defense workforce and education initiatives to attract and recruit leading talent in artificial intelligence and machine learning, including science, technology, engineering, and math programs;

(5) means by which the Department of Defense may establish data standards and provide incentives for the sharing of open training data; and

(6) any other matters the Secretary of Defense determines relevant with respect to the approach of the Department of Defense to artificial intelligence and machine learning.

(c) REPORTS.—

(1) INITIAL REPORT.—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 an initial report on the findings of the review required under subsection (a) and such recommendations as the Secretary may have for legislative action related to artificial intelligence, machine learning, and associated technologies, including recommendations to more effectively fund and organize the Department of Defense.

(2) COMPREHENSIVE REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a comprehensive report on the review required under subsection (a).

(d) DEFINITION OF ARTIFICIAL INTELLIGENCE.—In this section, the term ''artificial intelligence'' includes each of the following:

(1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.

(2) An artificial system developed in computer software, physical hardware, or other context that

solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.

(3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks.

(4) A set of techniques, including machine learning, that is designed to approximate a cognitive task.

(5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decisionmaking, and acting.

**SEC. 1053 [Log 67499]. REPORT ON PROPOSED CONSOLIDATION OF DEPARTMENT OF DEFENSE GLOBAL MESSAGING AND COUNTER MESSAGING CAPABILITIES.**

(a) REPORT REQUIRED.—The Secretary of Defense shall submit to the congressional defense committees a report on the proposed consolidation of the global messaging and counter messaging (GMCM) capabilities of the Department of Defense. Such report shall include each of the following:

(1) The justification of the Secretary for the proposed consolidation of such capabilities.

(2) The justification of the Secretary for the proposed designation of the United States Special Operations Command as the entity responsible for establishing the centralized GMCM capability.

(3) A description of the proposed roles and responsibilities of the United States Special Operations Command as such entity.

(4) A description of the roles and responsibilities of the combatant commanders regarding the operational use of the GMCM capability.

(5) The effect of the proposed consolidation of such capabilities on existing GMCM contracts and capabilities.

(6) An implementation plan that includes a detailed description of the resources and other requirements required for the United States Special Operations Command to establish the centralized GMCM capability for the period covered by the current future year's defense program.

(7) A comprehensive plan for the continual assessment of the effectiveness of the GMCM activities and programs.

(8) An identification of the anticipated efficiencies, cost savings, and operational benefits associated with the consolidation of the GMCM capabilities.

(9) A description of any actions, activities, and efforts taken to implement section 1637 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91).

(b) LIMITATION ON USE OF FUNDS.—Not more than 50 percent of the amounts authorized to be appropriated by this Act or otherwise made available for fiscal year 2019 for the Commander of the United States Special Operations Command for global messaging and counter messaging may be obligated or expended before the date that is 30 days after the date on which the Secretary submits the report required by subsection (a).

**SEC. 1054 [Log 67622]. COMPREHENSIVE REVIEW OF PROFESSIONALISM AND ETHICS PROGRAMS FOR SPECIAL OPERATIONS FORCES.**

(a) REVIEW REQUIRED.—The Secretary of Defense, in coordination with the Secretaries of each of the military departments, shall conduct a comprehensive review of the ethics and professionalism programs of the United States Special Operations Command and of the military departments for officers and other military personnel serving in special operations forces.

(b) ELEMENTS OF THE REVIEW.—The review conducted under subsection (a) shall specifically include a description and assessment of each of the following:

(1) The culture of professionalism and ethics of the United States Special Operations Command and affiliated component commands.

(2) The ethics and professionalism programs of the military departments available for special operations forces.

(3) The ethics and professionalism programs of the United States Special Operations Command and affiliated component commands.

(4) The roles and responsibilities of the military departments and the United States Special Operations Command and affiliated component commands in administering, overseeing, managing, and

ensuring compliance and participation of special operations forces in ethics and professionalism programs, including an identification of—

(A) gaps in the administration, oversight, and management of such programs and in ensuring the compliance and participation in such programs; and

(B) additional guidance that may be required for a systematic, integrated approach in administering, overseeing, and managing such programs and in ensuring compliance with and participation in such programs in order to address issues and improve ethical culture and professionalism.

(5) The management and oversight framework in place that is designed to ensure that all ethics and professionalism programs available to special operations forces meet Department standards.

(6) Tools and metrics for identifying and assessing individual and organizational ethics and professionalism issues with respect to special operations forces.

(7) Tools and metrics for assessing the effectiveness of existing ethics and professionalism programs in improving or addressing individual and or-

ganizational ethics-related and professionalism issues with respect to special operations forces.

(8) Additional programs or actions that may be required to address or improve individual and organizational ethics and professionalism issues with respect to special operations forces.

(9) Actions to improve the oversight and accountability by senior leaders of ethics and professionalism-related issues with respect to special operations forces.

(c) DEFINITIONS.—In this section:

(1) The term ''ethics program'' means a program that includes—

(A) compliance-based ethics training, education, initiative, or other activity that focuses on adherence to rules and regulations; and

(B) values-based ethics training, education, initiative, or other activity that focuses on upholding a set of ethical principles in order to achieve high standards of conduct and incorporate guiding principles to help foster an ethical culture and inform decision-making where rules are not clear.

(2) The term ''professionalism program'' means a program that includes training, education, initia-

tive, or other activity that focuses on values, ethics, standards, code of conduct, and skills as related to the military profession.

(d) SUBMITTAL OF REVIEW.—The Secretary of Defense shall submit the review required by subsection (a) to the Committees on Armed Services of the Senate and the House of Representatives by not later than March 1, 2019.

**SEC. 1062 [Log 67535]. PRINCIPAL ADVISOR ON COUNTERING WEAPONS OF MASS DESTRUCTION.**

(a) IN GENERAL.—

(1) DESIGNATION OF PRINCIPAL ADVISOR.—Chapter 4 of title 10, United States Code, is amended by adding at the end the following new section:

**"§ 145. Principal Advisor on Countering Weapons of Mass Destruction**

''(a) DESIGNATION.—The Secretary of Defense shall designate, from among the personnel of the Office of the Secretary of Defense, a Principal Advisor on Countering Weapons of Mass Destruction. Such Principal Advisor shall act as the principal advisor to the Secretary on the activities of the Department of Defense relating to countering weapons of mass destruction. The individual designated to serve as such Principal Advisor shall be an individual who was appointed to the position held by the individual by and with the advice and consent of the Senate.

''(b) RESPONSIBILITIES.—The Principal Advisor designated under subsection (a) shall carry out the following responsibilities:

''(1) Supervising the activities of the Department of Defense relating to countering weapons of mass destruction, including the oversight of policy and operational considerations, resources, personnel, acquisition, and technology.

''(2) Carrying out such other responsibilities relating to countering weapons of mass destruction as the Secretary shall specify.''.

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

''145. Principal Advisor on Countering Weapons of Mass Destruction.''.

(b) OVERSIGHT PLAN.—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 plan to streamline the oversight framework of the Office of the Secretary of Defense, including any efficiencies and the potential to reduce, realign, or otherwise restructure current Assistant Secretary and Deputy Assistant Secretary positions with responsibilities for overseeing countering weapons of mass destruction policy, programs, and activities.

**SEC. 1203. [LOG 67299] NATO STRATEGIC COMMUNICATIONS CENTER OF EXCELLENCE.**

(a) AUTHORIZATION.—The Secretary of Defense shall provide funds for the NATO Strategic Communications Center of Excellence (in this section referred to as the ''Center'') to—

(1) enhance the ability of military forces and civilian personnel of the countries participating in the Center to engage in joint strategic communications exercises or coalition or international military operations; and

(2) improve interoperability between the armed forces and the military forces of friendly foreign nations in the areas of strategic communications.

(b) CERTIFICATION.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall certify to the Committees on Armed Services of the House of Representatives and the Senate that the Secretary has assigned executive agent responsibility for the Center to an appropriate organization within the Department of Defense, and detail the steps being undertaken to strengthen the role of the Center in fostering strategic communications and information operations within NATO.

(c) BRIEFING REQUIREMENT.—The Secretary of Defense shall periodically brief the Committee on Armed

Services and the Committee on Foreign Relations of the Senate and the Committee on Armed Services and the Committee on Foreign Affairs of the House of Representatives on the efforts of the Department of Defense to strengthen the role of the Center in fostering strategic communications and information operations within NATO.

**SEC. 1204. [LOG 67298] NATO COOPERATIVE CYBER DEFENSE CENTER OF EXCELLENCE.**

(a) AUTHORIZATION.—The Secretary of Defense shall provide funds for the NATO Cooperative Cyber Defense Center of Excellence (in this section referred to as the ''Center'') to—

(1) enhance the ability of military forces and civilian personnel of the countries participating in the Center to engage in joint cyber exercises or coalition or international military operations; and

(2) improve interoperability between the armed forces and the military forces of friendly foreign countries in the areas of cyber and cybersecurity.

(b) CERTIFICATION.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall certify to the Committees on Armed Services of the House of Representatives and the Senate that the Secretary has assigned executive agent responsibilities for the Center to an appropriate organization within the Department of Defense, and detail the steps being undertaken to strengthen the role of the Center in fostering cyber defense and cyber warfare capabilities within NATO.

(c) BRIEFING REQUIREMENT.—The Secretary of Defense shall periodically brief the Committee on Armed Services and the Committee on Foreign Relations of the

Senate and the Committee on Armed Services and the Committee on Foreign Affairs of the House of Representatives on the efforts of the Department of Defense to strengthen the role of the Center in fostering cyber defense and cyber warfare capabilities within NATO.

**SEC. 1256. [LOG 67550] UNITED STATES-ISRAEL COUNTERING UNMANNED AERIAL SYSTEMS COOPERATION.**

Section 1279(a) of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 22 U.S.C. 8606 note), as most recently amended by section 1278 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 131 Stat. 1700), is further amended—

(1) by inserting ''and capabilities for countering unmanned aerial systems'' after ''anti-tunnel capabilities''; and

(2) by inserting ''and unmanned aerial systems'' after ''underground tunnels''.

**SEC. 1257. [LOG 67774] THREE-YEAR EXTENSION OF AUTHORIZATION OF NON-CONVENTIONAL ASSISTED RECOVERY CAPABILITIES.**

Section 943(g) of the National Defense Authorization Act for Fiscal Year 2009 (Public Law 110–417; 122 Stat. 4579), as most recently amended by section 1051(n) of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 131 Stat. 1564), is further amended by striking ''2021'' and inserting ''2024''.

**SEC. 1301.[Log 67547]. FUNDING ALLOCATIONS.**

Of the $335,240,000 authorized to be appropriated to the Department of Defense for fiscal year 2019 in section 301 and made available by the funding table in division D for the Department of Defense Cooperative Threat Reduction Program established under section 1321 of the Department of Defense Cooperative Threat Reduction Act (50 U.S.C. 3711), the following amounts may be obligated for the purposes specified:

(1) For strategic offensive arms elimination, $2,823,000.

(2) For chemical weapons destruction, $5,446,000.

(3) For global nuclear security, $29,001,000.

(4) For cooperative biological engagement, $197,585,000.

(5) For proliferation prevention, $74,937,000.

(6) For activities designated as Other Assessments/Administrative Costs, $25,448,000.

**SEC. 1302.[Log 67548]. SPECIFICATION OF COOPERATIVE THREAT REDUCTION FUNDS.**

Funds appropriated pursuant to the authorization of appropriations in section 301 and made available by the funding table in division D for the Department of Defense Cooperative Threat Reduction Program shall be available for obligation for fiscal years 2019, 2020, and 2021.

**SEC. 1413. [LOG 67212] QUARTERLY BRIEFING ON PROGRESS OF CHEMICAL DEMILITARIZATION PROGRAM.**

Section 1412(j) of the Department of Defense Authorization Act, 1986 (50 U.S.C. 1521(j)) is amended—

(1) in the heading, by striking ''Semiannual Reports'' and inserting ''QUARTERLY BRIEFING'';

(2) in paragraph (1)—

(A) by striking ''March 1'' and all that follows through ''the year in which'' and inserting ''90 days after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2019, and every 90 days thereafter until'';

(B) by striking ''submit to'' and inserting ''brief'';

(C) by striking ''a report on the implementation'' and inserting ''on the progress made''; and

(D) by striking ''of its chemical weapons destruction obligations'' and inserting ''toward fulfilling its chemical weapons destruction obligations''; and

(3) by striking paragraph (2) and inserting the following:

''(2) Each briefing under paragraph (1) shall include a description of contractor costs and per-

formance relative to schedule, the progress to date toward the complete destruction of the stockpile, and any other information the Secretary determines to be relevant.''.

☒

# Subtitle C—Cyberspace-Related Matters

**SEC. 1631.[Log 67337] AMENDMENTS TO PILOT PROGRAM REGARDING CYBER VULNERABILITIES OF DEPARTMENT OF DEFENSE CRITICAL INFRASTRUCTURE.**

Subsection (b) of section 1650 of the National Defense Authorization Act for Fiscal Year 2017 (10 U.S.C. 2224 note) is amended—

(1) in paragraph (1), in the matter preceding subparagraph (A), by inserting ''and the Defense Digital Service'' after ''covered research laboratory'';

(2) in paragraph (4), in the matter preceding subparagraph (A), by striking ''2019'' and inserting ''2020''; and

(3) in paragraph (5), by striking ''2019'' and inserting ''2020''.

**SEC. 1632.[Log 67647] BUDGET DISPLAY FOR CYBER VULNERABILITY EVALUATIONS AND MITIGATION ACTIVITIES FOR MAJOR WEAPON SYSTEMS OF THE DEPARTMENT OF DEFENSE.**

(a) BUDGET REQUIRED.—Beginning in fiscal year 2021 and in each fiscal year thereafter, the Secretary of Defense shall submit to Congress, as a part of the documentation that supports the President's annual budget for the Department of Defense, a consolidated Cyber Vulnerability Evaluation and Mitigation budget justification display for each major weapons system of the Department of Defense that includes the following:

(1) CYBER VULNERABILITY EVALUATIONS.—

(A) STATUS.—Whether, in accordance with paragraph (1) of section 1647(a) of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1118), the cyber vulnerability evaluation for each such major weapon system is pending, in progress, complete, or, pursuant to paragraph (2) of such section, waived.

(B) FUNDING.—The funding required for the fiscal year with respect to which the budget is submitted and for at least the four succeeding fiscal years required to complete the

pending or in progress cyber vulnerability evaluation of each such major weapon system.

(C) DESCRIPTION.—A description of the activities planned in the fiscal year with respect to which the budget is submitted and at least the four succeeding fiscal years to complete the required evaluation for each such major weapon system.

(D) RISK ANALYSIS.—An description of operational or security risks associated with cyber vulnerabilities identified as a result of such cyber vulnerability evaluations that require mitigation.

(2) MITIGATION ACTIVITIES.—

(A) STATUS.—Whether activities to address identified cyber vulnerabilities of such major weapon systems resulting in operational or security risks requiring mitigation are pending, in progress, or complete.

(B) FUNDING.—The funding required for the fiscal year with respect to which the budget is submitted and for at least the four succeeding fiscal years required to complete the pending or in progress mitigation activities re-

ferred to in subparagraph (A) related to such major weapon systems.

(C) DESCRIPTION.—A description of the activities planned in the fiscal year with respect to which the budget is submitted and at least the four succeeding fiscal years to complete any necessary mitigation.

(b) FORM.—The display required under subsection (a) shall be submitted in an unclassified form, but may include a classified annex if necessary.

**SEC. 1633.[Log 67358] TRANSFER OF RESPONSIBILITY FOR THE DEPARTMENT OF DEFENSE INFORMATION NETWORK TO UNITED STATES CYBER COMMAND.**

(a) IN GENERAL.—Not later than September 30, 2019, the Secretary of Defense shall transfer all roles, missions, and responsibilities of the Commander, Joint Force Headquarters - Department of Defense Information Networks (JFHQ–DODIN) from the Defense Information Support Agency to the Commander, United States Cyber Command.

(b) CERTIFICATION REQUIRED.—Prior to the transfer required under subsection (a), the Secretary of Defense shall certify in writing to the congressional defense committees that such transfer shall not result in mission degradation.

**SEC. 1634.[Log 67332] PILOT PROGRAM AUTHORITY TO ENHANCE CYBERSECURITY AND RESILIENCY OF CRITICAL INFRASTRUCTURE.**

(a) AUTHORITY.—The Secretary of Defense, in coordination with the Secretary of Homeland Security, is authorized to provide, detail, or assign technical personnel to the Department of Homeland Security on a non-reimbursable basis to enhance cybersecurity cooperation, collaboration, and unity of Government efforts.

(b) SCOPE OF ASSISTANCE.—The authority under subsection (a) shall be limited in any fiscal year to the provision of not more than 50 technical cybersecurity personnel from the Department of Defense to the Department of Homeland Security, including the national cybersecurity and communications integration center (NCCIC) of the Department, or other locations as agreed upon by the Secretary of Defense and the Secretary of Homeland Security.

(c) LIMITATION.—The authority under subsection (a) may not negatively impact the primary missions of the Department of Defense or the Department of Homeland Security.

(d) ESTABLISHMENT OF PROCEDURES.—

(1) IN GENERAL.—The Secretary of Defense and the Secretary of Homeland Security shall establish procedures to carry out subsection (a), including

procedures relating to the protection of and safeguards for maintenance of information held by the NCCIC regarding United States persons.

(2) LIMITATION.—Nothing in this subsection may be construed as providing authority to the Secretary of Defense to establish procedures regarding the NCCIC with respect to any matter outside the scope of this section.

(e) NO EFFECT ON OTHER AUTHORITY TO PROVIDE SUPPORT.—Nothing in this section may be construed to limit the authority of an Executive department, military department, or independent establishment to provide any appropriate support, including cybersecurity support, or to provide, detail, or assign personnel, under any other law, rule, or regulation.

(f) DEFINITIONS.—In this section, each of the terms ''Executive department'', ''military department'', and ''independent establishment'', has the meaning given each of such terms, respectively, in chapter 1 of title 5, United States Code.

(g) TERMINATION OF AUTHORITY.—This section shall terminate on September 30, 2022.

**SEC. 1635.[Log 67333] PROCEDURES AND REPORTING REQUIREMENT ON CYBERSECURITY BREACHES AND LOSS OF PERSONALLY IDENTIFIABLE INFORMATION.**

(a) IN GENERAL.—In the event of a significant loss of personally identifiable information of civilian or uniformed members of the Armed Forces, the Secretary of Defense shall promptly submit to the congressional defense committees notice in writing of such loss. Such notice may be submitted in classified or unclassified formats.

(b) PROCEDURES.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall establish and submit to the congressional defense committees procedures for complying with the requirements of subsection (a). Such procedures shall be consistent with the national security of the United States, the protection of operational integrity, and the protection of personally identifiable information of civilian and uniformed members of the Armed Forces.

(c) SIGNIFICANT LOSS OF PERSONALLY IDENTIFIABLE INFORMATION DEFINED.—In this section, the term ''significant loss of personally identifiable information'' means an intentional, accidental, or otherwise known disclosure of information that can be used to distinguish or trace an individual's identity, such as the name, social security number, date and place of birth, biometric records,

home or other phone numbers, or other demographic, personnel, medical, or financial information, involving 250 or more civilian or uniformed members of the Armed Forces.

**SEC. 1636.[Log 67302]. STUDY AND REPORT ON RESERVE COMPONENT CYBER CIVIL SUPPORT TEAMS.**

(a) STUDY REQUIRED.—The Secretaries concerned shall conduct a study on the feasibility, advisability, and necessity of the establishment of reserve component cyber civil support teams for each State.

(b) ELEMENTS.—The study under subsection (a) shall include the following:

(1) An examination of the potential ability of the teams referred to in such subsection to respond to an attack, natural disaster, or other large-scale incident affecting computer networks, electronics, or cyber capabilities.

(2) An analysis of State and local civilian and private sector cyber response capabilities and services, including an identification of any gaps in such capabilities and services.

(3) An identification of the potential role of such teams with respect to the principles and processes set forth in—

(A) Presidential Policy Directive 20 (United States Cyber Operations Policy);

(B) Presidential Policy Directive 21 (Critical Infrastructure Security and Resilience); and

(C) Presidential Policy Directive 41 (United States Cyber Incident Coordination).

(4) An explanation of how such teams may interact with other organizations and elements of the Federal Government that have responsibilities under the Presidential Policy Directives referred to in paragraph (5).

(5) The amount of funding and other resources that may be required by the Department of Defense to organize, train, and equip such teams.

(6) An explanation of how the establishment of such teams may affect the ability of the Department of Defense—

(A) to organize, train, equip, and employ the Cyber Mission Force, and other organic cyber forces; and

(B) to perform national defense missions and defense support to civil authorities for cyber incident response.

(7) An explanation of how the establishment of such teams may affect the ability of the Department of Homeland Security—

(A) to organize, train, equip, and employ cyber incident response teams; and

(B) to perform civilian cyber response missions.

(8) Any effects on the privacy and civil liberties of United States persons that may result from the establishment of such teams.

(9) Any other considerations determined to be relevant by the Secretaries concerned.

(c) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretaries concerned shall submit to the appropriate congressional committees a report that includes—

(1) the results of the study conducted under subsection (a), including an explanation of each element described in subsection (b);

(2) the final determination of the Secretaries with respect to the feasibility, advisability, and necessity of establishing reserve component cyber civil support teams for each State; and

(3) if such final determination is in the affirmative, proposed legislation for the establishment of the teams, which may include proposed legislation to amend section 12310 of title 10, United States Code.

(d) DEFINITIONS.—In this section:

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

(A) the congressional defense committees;

(B) the Committee on Homeland Security of the House of Representatives; and

(C) the Committee on Homeland Security and Governmental Affairs of the Senate.

(2) The term ''reserve component cyber civil support team'' means a team that—

(A) is comprised of members of the reserve components;

(B) is organized, trained, equipped, and sustained by the Department of Defense for the purpose of assisting State authorities in preparing for and responding to cyber incidents, cyber emergencies, and cyber attacks; and

(C) operates principally under the command and control of the Chief Executive of the State in which the team is located.

(3) The term ''Secretaries concerned'' means the Secretary of Defense and the Secretary of Homeland Security acting jointly.

(4) The term ''State'' means each of the several States, the District of Columbia, the Commonwealth of Puerto Rico, and the United States Virgin Islands.

# DIRECTIVE REPORT LANGUAGE

# Table Of Contents

# DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

## TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

### RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, ARMY

Items of Special Interest

*Urban warfare training*

The committee has continuing interest in the Department of Defense's ability to prepare for and operate in complex, densely populated urban terrain. Recent trends reflect that the future of global violence is urban, and that the next war will likely be fought in densely populated cities. The committee is supportive of the Department's ongoing efforts, but remains concerned with the lack of Army prioritization and resourcing to address these challenges. The committee is particularly concerned with the Army's lack of realistic training sites that reflect the scale and density of real-world urban operating environments. The committee believes the Army should more aggressively prepare for urban warfare and explore the construction of an urban warfare training center that focuses on basic and advanced skills to fight, survive, and win in urban operating environments. This training should address the challenges associated with vertical, subterranean, and dense urban terrain, and the inclusion and integration of joint and interagency enablers.

Therefore, the committee directs the Secretary of the Army to provide a briefing to the House Committee on Armed Services not later than February 1, 2019, on the Army's plan for urban warfare training. The report should include:

(1) a description of urban warfare training requirements;

(2) an overview of a plan and timeline to integrate urban warfare training within the Army;

(3) an identification of costs associated with an urban warfare training program;

(4) a feasibility study on the construction of an urban warfare training center;

(5) any critical technology, maneuver, or mobility shortfalls associated with operating in a dense urban environment; and

(6) force design impacts or considerations within the Army.

### RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, DEFENSE-WIDE

Items of Special Interest

*Counter-unmanned aerial system threat detection*

The committee is interested in advancements in counter-unmanned aerial system (C-UAS) technology and the threat these systems pose to the Armed Forces. The committee supports ongoing efforts by the U.S. Army and U.S. Special Operations Command to develop and employ unmanned aerial system (UAS) threat detection technology, and commends the services for recognizing the seriousness of the threat. In light of recent UAS attacks in the U.S. Central Command area of responsibility, the committee is concerned about the increased threat from unmanned aerial systems to forward operating bases and special operations forces personnel. The committee believes additional advancements in scalable C-UAS technologies are necessary to effectively detect, track, neutralize, and ensure the force protection and operational security of deployed service members.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by October 31, 2018, on the employment of C-UAS systems. The briefing should include an assessment of the UAS threat to the Armed Forces, a roadmap for C-UAS threat detection technology and capabilities, and the results of operational fielding of C-UAS systems.

*Future uses of synthetic biology*

The committee is aware of recent advancements in synthetic biology, genomics, biotechnology, and related novel technologies that may enhance human performance and improve traditional approaches to healthcare. This includes enhancing human ability to perform through stressful and resource-limited environments, improving decision making, minimizing the time between disease identification and treatment, and augmenting human immune systems to defeat a variety of diseases, rather than depending on specific vaccines and therapeutics. The development of advanced biosensors to understand hypoxia is a current example of the type of human performance challenges that can be addressed through these advancements.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by December 1, 2018, on how the Department of Defense may leverage these advancements, when appropriate, and in accordance with ethical standards, U.S. law, our nation's values, and Department of Defense policy, to enhance service members' performance, increase lethality and survivability, and improve battlefield healthcare. The briefing should also identify opportunities, when appropriate and feasible, to facilitate the maturation of capabilities based on recent advancements.

*Innovative installation capabilities*

The budget request contained $29.4 million in PE 63342D8W for the Defense Innovation Unit Experimental (DIUx).

DIUx supports the identification, development, and demonstration of game-changing technologies to satisfy joint force priorities at a faster pace than the traditional Department of Defense planning, programming, budgeting, and execution process. As DIUx leverages partnerships with academic institutions, science and technology communities, and private industries, the committee recognizes the advantages that DIUx may provide to accelerate fielding of decisive technical capabilities and interoperability while mitigating operational risk to the warfighter and promoting affordability.

The committee supports the objective of DIUx to maintain U.S. technological superiority across the range of military operations. The committee believes DIUx should also increase efforts to support technological superiority at Department installations by addressing critical technological needs. This may also include mitigation of cybersecurity vulnerabilities identified during the ongoing review of critical infrastructure being conducted by the Department as directed in section 1650 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328).

Therefore, the committee recommends prioritizing critical technological needs at Department installations, and directs the Director of DIUx to provide a briefing to the House Committee on Armed Services by October 1, 2018, on a plan to invest in the rapid insertion of innovative installation capabilities.

*Military Free Fall School*

The committee is aware of the increased demand being placed on the U.S. Army's Military Free Fall School (MFFS). The committee understands the increased student throughput is largely a result of the expanded population of U.S. Army Special Operations Command personnel who are required to attend MFFS. Consequently, the increased student throughput has resulted in shortfalls in resourcing, an over-reliance on contract personnel, and an increased risk to students and cadre. Therefore, the committee directs the Commander, U.S. Special Operations Command to provide a briefing to the House Committee on Armed Services not later than October 15, 2018, on Special Operations Force Military Free Fall requirements, the funds expended, the expected cost of operating the MFFS across the Future Years Defense Program, and any change in the rate of MFFS safety incidents or injuries from fiscal years 2012 through 2018.

*National Hypersonics Initiative*

The committee is aware of a National Hypersonics Initiative under development by the Under Secretary of Defense for Research and Engineering, in conjunction with the military services, defense labs, and the Defense Advanced Research Projects Agency. The committee recognizes the growing amount of resources and emphasis placed by the Department of Defense on the research and development of hypersonic vehicle technology. The committee supports the development of a National Hypersonics Initiative, and believes it is prudent and

consistent with the roles and responsibilities granted to the Department's Joint Hypersonics Transition Office as authorized in the National Defense Authorization Act of 2018 (Public Law 115-91).

Therefore, the committee directs the Under Secretary of Defense for Research and Engineering to provide a briefing to the House Committee on Armed Services not later than September 15, 2018, on the status of the National Hypersonics Initiative.

*National lab integration in defense innovation hubs*

The committee has continuing interest in the Department of Defense laboratories and engineering centers, their responsiveness to Department of Defense requirements, and maximizing their expertise and reach. The Department's laboratories are integral to the Department's ability to retain capability in areas where the private sector has no commercial interest, and ensuring that commercial solutions are adapted for warfighter needs in a timely manner so that the United States remains dominant in the land, air, sea, space, and cyber domains.

The committee recommends that the Department better enable laboratories and centers to embrace an open and innovative posture, while simultaneously becoming more active in the Department's requirements process. The committee is aware of the Army Research Lab's Open Campus project as an example of open innovation that encourages groundbreaking advances in basic and applied research areas through increased collaboration with the broader research enterprise. The committee believes that this serves as a model for laboratories to become more ingrained in the scientific and research communities, both locally and globally, and become a greater sensor for disruptive technologies that present opportunities or highlight vulnerabilities for the Department. Additionally, the committee recommends that the laboratories increase their presence in innovation hubs across the United States, like those established by the Defense Innovation Unit Experimental, and enhance existing relationships with the Strategic Capabilities Office and the Defense Advanced Research Projects Agency.

Therefore, the committee directs the Under Secretary of Defense for Research and Engineering to provide a briefing to the House Committee on Armed Services not later than October 1, 2018, on the respective plan for further integrating the laboratories across defense and commercial innovation hubs, and maximizing their expertise and reach. The briefing should include a robust plan and timeline for increasing the Department's laboratory joint presence in innovation hubs across the United States.

# TITLE V—MILITARY PERSONNEL POLICY

## ITEMS OF SPECIAL INTEREST

### U.S. Special Operations Command Preservation of the Force and Families Program Contract Support

The committee recognizes that U.S. special operations forces (SOF) and their families are under unique and continued stresses, including psychological, social, spiritual, and human performance strains. The committee commends the success of the Preservation of the Force and Family (POTFF) program. It has helped to alleviate the magnitude of these stresses and break the stigma of seeking necessary help. It has also decreased rehabilitation time following physical injuries.

The committee understands U.S. Special Operations Command (SOCOM) and component commands have engaged in dialogue with the military services on scaling portions of the program to the broader force. The committee supports this dialogue and encourages the transition by SOCOM of resources and management for aspects of POTFF that are scaled to the military services , as well as a continual assessment of what remain as SOF-specific needs.

However, with POTFF's contract due to expire this fiscal year, the committee is concerned by the request for proposal submitted by SOCOM. It once again indicates a domineering focus on human performance, to the detriment of a distinct emphasis on mental, emotional, and behavioral health. The committee notes that of the $88.0 million for POTFF in the budget request for fiscal year 2019, only $13.0 million was to support the Psychological Performance Program to promote, maintain, and restore the psychological and behavioral health of SOF.

With these concerns in mind, the committee directs the Commander of Special Operations Command, in coordination with the Secretary of Defense, to provide a briefing to the House Committee on Armed Services by September 14, 2018, on the future of POTFF. The briefing shall include:

(1) how the command plans to balance the emphasis put on the four pillars of the program;

(2) an analysis of mental and behavioral health program gaps, to include an in-depth look into POTFF's suicide-prevention programming; and

(3) how SOCOM will work with services to identify successful elements that can be transitioned to assist conventional forces and families.

## TITLE X—GENERAL PROVISIONS

### ITEMS OF SPECIAL INTEREST

#### OTHER MATTERS

### Assessment of Air National Guard and Air Force Reserve Involuntary Mobilization Plans to Support Special Operations Activities

During review of the fiscal year 2019 President's budget request and related activities in support of Air Force Special Operations Command (AFSOC),

the committee determined that a small number of Air National Guard units and all Air Force Reserve Command units that support AFSOC missions and force presentation requirements do not possess a current, validated involuntary mobilization plan that complies with various Department of Defense, Department of the Air Force, and Special Operations Command instructions or policies. The committee is concerned that without sufficient and validated involuntary mobilization plans that detail how the Air National Guard and the Air Force Reserve Command intend to support AFSOC as operational reserve units, should the need arise for Special Operations Command to fully mobilize forces in support of global special operations activities, the Air National Guard and Air Force Reserve Command may lack the capability and capacity to support the mission.

Therefore, the committee directs the Comptroller General of the United States to provide a briefing to the House Committee on Armed Services not later than March 1, 2019, that assesses involuntary mobilization plans for Air National Guard and Air Force Reserve Command units that support Air Force Special Operations missions and activities. The Comptroller General should assess, at a minimum:

(1) the existence and recency of an involuntary mobilization plan;

(2) the sufficiency and validity of the plan as compared to a unit's Designed Operational Capability statement, authorized and assigned manpower levels, authorized and assigned equipment, facilities, and support functions necessary to execute the plan;

(3) comparison with existing Department of Defense policy and regulations governing mobilization-to-dwell and deployment-to-dwell goals and objectives;

(4) any discrepancies, shortfalls, or gaps associated with the aforementioned areas of assessment; and

(5) any additional information the Comptroller General would find useful to support the briefing.

Civil Support Team Information Management System

The committee is aware that the National Guard Bureau Weapons of Mass Destruction Civil Support Teams (CST) currently field the CST Information Management System (CIMS). CIMS provides a common operation picture and promotes information sharing and real-time collaboration. CIMS also supports the CST mission of assisting and advising first responders and facilitating communications with other Federal resources in an emergency.

The committee encourages the expansion of CIMS to establish an enterprise-wide capable tool, commonly referred to as the National Guard Chemical, Biological, Radiological, and Nuclear Response Enterprise Information Management System 2018+ (NG CIMS 2018+). The committee believes that expansion will increase the capabilities of the CIMS to support other National Guard Bureau forces, such as the Chemical, Biological, Radiological, Nuclear, and

High-Explosive Enhanced Response Force Package and Homeland Defense Response Force units.

The committee notes that the timeline the Department of Defense previously presented to the committee in their September 8, 2015, report "Civil Support Team Information Management System" has been delayed. The committee, therefore, directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by October 1, 2018, on the plan for the development of NG CIMS 2018+, including a description of timelines, milestones, fielding, and completion dates.

### Counterterrorism Effectiveness Research

The committee recognizes that basic research into the effectiveness of current counterterrorism policies and strategy is critical to informing and shaping future efforts. The committee understands that there is currently a wide range of social science research in these areas that should be leveraged, including better use of and integration with existing research by organizations maintaining databases of terrorism incidents globally.

For example, the National Consortium for the Study of Terrorism and Responses to Terrorism (START) is a university-based research and education center. The center is comprised of an international network of scholars committed to the scientific study of the causes and human consequences of terrorism in the United States and around the world. START supports the research efforts of leading social scientists at more than 50 academic and research institutions across the country and the globe.

The committee is aware the START program supports more than 14 terrorism and counterterrorism related datasets that are used across civilian and defense agencies, including the Department of Homeland Security and the Department of Defense, in order to directly inform international, Federal, State, and local training and educational programs.

However, the budget request for fiscal year 2019 did not include funding for this effort. The committee believes that it is within the purview of the Department of Defense, and specifically U.S. Special Operations Command (SOCOM) as the Coordinating Authority for Countering Violent Extremist Organizations, to foster academically rigorous studies of terrorism, like the START initiative, to provide a foundational understanding for how to assess the effectiveness of specific counterterrorism activities and programs, and best practices to inform counterterrorism policies. Further, the committee believes that as the Coordinating Authority for Countering Weapons of Mass Destruction (CWMD), SOCOM may also derive similar benefits for the Department of Defense from research pertaining to CWMD strategies, policies, and programs, by leveraging and enhancing programs like START.

Therefore, the committee directs the Commander, U.S. Special Operations Command to provide a briefing to the House Committee on Armed Services by

October 30, 2018, on the feasibility and advisability of funding programs like START.

### Genetic and Medical Information Security

Recent advancements in information and computational capabilities, along with advancements in synthetic biology and genomics, have resulted in the convergence of data and life sciences. The committee is troubled by the potential risks posed by the proliferation of personal biological information, including DNA sequences, electronic medical records, medical claims processing data, pharmacy records, health information exchanges, and activity trackers. The committee recognizes this information is essential for the development of precision medicine, but is concerned about the potential lack of appropriate security control over the data of service members due to the growing efforts by adversaries to acquire this information. The committee believes acquisition of this information by adversaries may lead to the development of new biological threats.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by March 1, 2019, on the Department of Defense's effort to secure service members' genetic, medical, and lifestyle information. The briefing shall include information on the location, access control, and security protocols of all databases with this information; and offer policy recommendations for protecting this information.

The committee further directs the Director of the Defense Intelligence Agency to provide a briefing to the House Committee on Armed Services by March 1, 2019, on foreign intelligence services attempts to collect this information on Department of Defense personnel, including:

(1) attempts by foreign intelligence services to collect genetic data, medical records, and any other personal health or biological information;

(2) use of non-traditional intelligence collection techniques, to include foreign investment in commercial entities that offer genetic data analysis, medical record administration, and other health information services; and

(3) use of this data lost through data breaches, unauthorized disclosures, or non-traditional collection techniques to enable targeting of U.S. persons.

### MQ-9 Enterprise Supporting Air Combat Command and Air Force Special Operations Command Activities

After a detailed review, the committee has determined that a system to manage and develop MQ-9 specific remotely piloted aircraft (RPA) aircrews does not exist between Air Force Special Operations Command (AFSOC), Air Combat Command (ACC), and the Air Force Personnel Center. The committee is concerned that ACC is the Air Force's primary entity responsible for managing, assigning, and transitioning MQ-9 aircrews for AFSOC and that AFSOC may not have the visibility it needs into ACC "talent management" processes to sufficiently support AFSOC future planning and normalization of operations tempo. Moreover, the role

of the Air Force Personnel Center's in managing and career-shaping MQ-9 aircrews is unclear.

Therefore, the committee directs the Commander of ACC, in cordination with the Commander of AFSOC and the Commander of the Air Force Personnel Center, to provide a briefing to the House Committee on Armed Services not later than October 19, 2018, on how MQ-9 aircrews are assigned, managed, and developed among ACC and AFSOC. The briefing should also include an update regarding the Air Force's MQ-9 Culture and Process Improvement Program activities for each command, and each command's progress for acquiring the necessary manpower authorizations, and actual assigned manpower, to achieve deployment to dwell operations tempo to comply with Department of Defense policies.

## Preparedness of U.S. Forces to Counter North Korean Chemical and Biological Weapons

The committee is aware of reports of the Democratic People's Republic of Korea's pursuit of the essential laboratories, equipment, and skills for an advanced biological weapons program, in addition to reports of existing stockpiles of chemical weapons. The 2017 National Security Strategy states that North Korea is pursuing chemical and biological weapons, which could be delivered by missile. The strategy also states that the Department of Defense will ensure U.S. military forces can operate effectively in the face of biological weapons attacks, and that our troops and critical domestic and overseas installations are effectively protected against such threats.

To assist the committee in conducting its oversight of the preparedness of U.S. forces to respond to these threats, the committee directs the Comptroller General of the United States to review the extent to which Department of Defense military units deployed to the Republic of Korea and the Department's chemical and biological defense support units on the Korean peninsula, in the U.S. Pacific Command area of responsibility, and in the United States, are prepared to counter chemical and biological weapons, including:

(1) detection and identification;

(2) individual and collective protection;

(3) medical countermeasures;

(4) decontamination;

(5) training and exercises; and

(6) any other matters the Comptroller General deems relevant.

The committee also directs the Comptroller General to provide a briefing to the House Committee on Armed Services by March 1, 2019, on the preliminary results of the review, and submit a subsequent report by a date agreed to at the time of the briefing.

# TITLE XIII—COOPERATIVE THREAT REDUCTION

## ITEMS OF SPECIAL INTEREST

### Future of the Cooperative Threat Reduction Program

The committee notes the successful history of the Nunn-Lugar Cooperative Threat Reduction (CTR) program, including the pivotal role it played in securing former Soviet Union nuclear material and delivery platforms, the destruction of Russian and Syrian chemical weapons, and the securing of sensitive biological laboratories around the world. In response to an evolving threat landscape, Congress has provided modifications to the original program to address current requirements for threat reduction and the proliferation of weapons of mass destruction (WMD) by state and non-state actors around the globe.

The committee is aware that additional opportunities may exist for enhanced cooperation with allies and partners to address emerging proliferation concerns and WMD threats, such as those on the Korean Peninsula. The committee notes, however, that interagency coordination, expeditious project approval, prioritization, measuring program effectiveness, and policy gaps continue to pose challenges to effective and efficient utilization of CTR by the Department of Defense, despite efforts for improvement.

Therefore, the committee directs the Secretary of Defense to provide a report to the House Committee on Armed Services by December 1, 2018, on how to strengthen the CTR program so that it may be better leveraged for emerging threat reduction and proliferation concerns in an efficient and expeditious manner.

# TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

## ITEMS OF SPECIAL INTEREST

### CYBER-RELATED MATTERS

### Comptroller General Review of Current Military Cyber Operations

The committee notes that in the last several years, the Department of Defense has employed cyber capabilities to achieve objectives in or through cyberspace. Unlike military operations that occur in the air and land domains, cyberspace operations and the effects of those operations are not always visible to Congress and the American people. The committee believes that as the Department continues to conduct cyberspace operations, it will be critical that operations are fully aligned with the appropriate authorities, policies and doctrine, rules of engagement, plans, oversight mechanisms, and lessons learned processes. It will also be important that the Department manages the number of organizations that

are conducting these operations, to ensure there are clearly defined roles and responsibilities, and that there are deconfliction mechanisms in place.

Therefore, the committee directs the Comptroller General of the United States to assess the Department of Defense's current military cyberspace operations. The assessment should identify:

(1) the types of cyberspace operations the Department has undertaken, activities undertaken to prepare for cyberspace operations, and the organizations conducting these operations;

(2) authorities, policies, doctrine, and rules of engagement for these operations;

(3) internal oversight and congressional reporting mechanisms;

(4) efforts to develop and synchronize cyberspace operations within combatant commanders' plans; and

(5) processes used to deconflict cyberspace operations or mitigate the impact of cyberspace operations on other military operations.

The committee directs the Comptroller General to provide a briefing to the House Committee on Armed Services by March 1, 2019, on preliminary findings, and submit a final report to the congressional defense committees at a date agreed to at the time of the briefing.

Comptroller General Review of Information Operations Strategy

The committee notes that information operations are a means for the United States to promote economic and political freedom, as well as countering all forms of extremism and adversarial influence. In June 2016, in response to a congressional requirement, the Department of Defense issued an information operations strategy to align departmental actions and ensure effective integration of Department of Defense efforts. These efforts contribute to the mission that the Department of State's Global Engagement Center was directed to lead, organize, and synchronize.

Section 1637 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115-91) directed the Department of Defense to establish processes and procedures to integrate strategic information operations and cyber-enabled information operations across the relevant elements of the Department of Defense, including those responsible for military deception, public affairs, electronic warfare, and cyber operations. This section also directed the Department of Defense to coordinate regional information strategies and interagency coordination plans of the combatant commands with the appropriate Department of State officials and the Global Engagement Center, and to develop an implementation plan to support the Department of Defense Strategy for Operations in the Information Environment. However, the committee remains concerned about the lack of progress in developing the strategy, tools, and coordination mechanisms to counter adversarial influence.

Therefore, the committee directs the Comptroller General of the United States to assess the Department's information operations strategy and implementation efforts. The assessment shall:

(1) identify the Department of Defense's implementation of the 2016 strategy, integration of cyber and intelligence capabilities, and other activities, for information operations;

(2) identify roles, responsibilities, and coordination of activities within the Department of Defense, and between the Department and interagency partners;

(3) identify previous and planned investments by the Department to support and implement information operations; and

(4) any other matters the Comptroller General determines relevant.

The committee directs the Comptroller General to provide a briefing to the House Committee on Armed Services by March 1, 2019, on preliminary findings, with a report to follow at a time agreed to at the time of the briefing.

## INTELLIGENCE MATTERS

### Insider Threat Detection and User Activity Monitoring

The committee is aware that in June 2015, the Government Accountability Office recommended that the Department of Defense issue risk-assessment guidance and evaluate the ability of its insider threat programs to address capability gaps (GAO-15-544). The committee is also aware of the Department's efforts to rapidly detect and remedy cyber vulnerabilities through programs such as the Air Force's Automated Remediation and Asset Discovery Program. The committee believes that continuous network monitoring and greater network visibility can significantly improve security of the Department's classified information and systems. Therefore, the committee encourages the Department to perform cost and technical analyses of available commercial off-the-shelf and government off-the-shelf solutions for user activity monitoring and for rapid detection and remediation of cyber attacks, for the purposes of obtaining best value and performance to decrease risks.

Further, the committee directs the Chief Management Officer to provide a briefing to the House Committee on Armed Services by November 1, 2018, on the outcomes of its cost and technical analyses required by this report, and the Department's efforts to implement enterprise-wide programs and policies for insider threat detection, user activity monitoring, and cyber attack detection and remediation.