

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

**SUBCOMMITTEE ON EMERGING
THREATS AND CAPABILITIES**

SUMMARY OF BILL LANGUAGE.....	1
BILL LANGUAGE.....	11
DIRECTIVE REPORT LANGUAGE	65

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 2XX—Plan for Elimination or Transfer of the Strategic Capabilities
Office of the Department of Defense

Section 2XX—Extension of Directed Energy Prototyping Authority

Section 2XX—Modification of Authority to Carry Out Certain Prototype
Projects

Section 2XX—Limitation on Availability of Funds for Certain High Energy
Laser Advanced Technology

SUBTITLE C—REPORTS AND OTHER MATTERS

Section 2xx—Briefing on Use of 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 5xx—Enhancement and Clarification of Family Support Services for
Family Members of Members of Special Operations Forces

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

LEGISLATIVE PROVISIONS

SUBTITLE B—ACQUISITION CLARITY

Section 8XX—Consolidated Budget Justification for the Department of
Defense Small Business Innovation Research Program and Small Business
Technology Transfer Program

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

LEGISLATIVE PROVISIONS

SUBTITLE A—ORGANIZATION AND MANAGEMENT OF THE DEPARTMENT OF DEFENSE GENERALLY

Section 9XX—Artificial Intelligence and Machine Learning Policy and
Oversight Council

TITLE X—GENERAL PROVISIONS

LEGISLATIVE PROVISIONS

SUBTITLE D—COUNTERTERRORISM

Section 10XX—Definition of Sensitive Military Operation

SUBTITLE G—OTHER MATTERS

Section 10XX—Department of Defense Review and Assessment on Advances in Artificial Intelligence and Machine Learning

Section 10XX—Report on Proposed Consolidation of Department of Defense Global Messaging and Counter Messaging Capabilities

Section 10XX—Principal Advisor on Countering Weapons of Mass Destruction

Section 10XX—Comprehensive Review of Professionalism and Ethics Programs for Special Operations Forces

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

LEGISLATIVE PROVISIONS

SUBTITLE F—OTHER MATTERS

Section 12XX—Three-Year Extension of Authorization of Non-Conventional Assisted Recovery Capabilities

Section 12XX—NATO Cooperative Cyber Defense Center of Excellence

Section 12XX—NATO Strategic Communications Center of Excellence

Section 12xx—United States-Israel Countering Unmanned Aerial Systems Cooperation

TITLE XIII—COOPERATIVE THREAT REDUCTION

LEGISLATIVE PROVISIONS

Section 13xx—Funding Allocations

Section 13XX—Specification of Cooperative Threat Reduction Funds

TITLE XIV—OTHER AUTHORIZATIONS

LEGISLATIVE PROVISIONS

SUBTITLE A—MILITARY PROGRAMS

Section 14xx—Quarterly Briefing on Progress of Chemical Demilitarization Program

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE D—CYBERSPACE-RELATED MATTERS

Section 16XX—Study and Report on Reserve Component Cyber Civil Support Teams

Section 16XX—Pilot Program Authority to Enhance Cybersecurity and Resiliency of Critical Infrastructure

Section 16XX—Procedures and Reporting Requirement on Cybersecurity Breaches and Loss of Personally Identifiable Information

Section 16XX—Amendments to Pilot Program Regarding Cyber Vulnerabilities of Department of Defense Critical Infrastructure

Section 16XX—Transfer of Responsibility for the Department of Defense Information Network to United States Cyber Command

Section 16XX—Budget Display for Cyber Vulnerability Evaluations and Mitigation Activities for Major Weapon Systems of the Department of Defense

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

LEGISLATIVE PROVISIONS

SUBTITLE B—PROGRAM REQUIREMENTS, RESTRICTIONS, AND LIMITATIONS

Section 2XX—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.

Section 2XX—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 2XX—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 2XX—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.

SUBTITLE C—REPORTS AND OTHER MATTERS

Section 2xx—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 5xx—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 B—ACQUISITION CLARITY

Section 8XX—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 A—ORGANIZATION AND MANAGEMENT OF THE DEPARTMENT OF DEFENSE GENERALLY

Section 9XX—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 10XX—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 G—OTHER MATTERS

Section 10XX—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 10XX—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 10XX—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.

Section 10XX—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.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

LEGISLATIVE PROVISIONS

SUBTITLE F—OTHER MATTERS

Section 12XX—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”.

Section 12XX—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.

Section 12XX—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 12xx—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.

TITLE XIII—COOPERATIVE THREAT REDUCTION

LEGISLATIVE PROVISIONS

Section 13xx—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 13XX—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 A—MILITARY PROGRAMS

Section 14xx—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 D—CYBERSPACE-RELATED MATTERS

Section 16XX—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.

Section 16XX—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 16XX—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 16XX—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 16XX—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 16XX—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.

BILL LANGUAGE

1 **SEC. 2** [Log 67335]. **PLAN FOR ELIMINATION OR TRANS-**
2 **FER OF THE STRATEGIC CAPABILITIES OF-**
3 **OFFICE OF THE DEPARTMENT OF DEFENSE.**

4 (a) **PLAN REQUIRED.**—Not later than March 1,
5 2019, the Secretary of Defense, acting through the Under
6 Secretary of Defense for Research and Engineering, shall
7 submit to the congressional defense committees a plan—

8 (1) to eliminate the Strategic Capabilities Office
9 of the Department of Defense by not later than Oc-
10 tober 1, 2020; or

11 (2) to transfer the functions of the Strategic
12 Capabilities Office to another organization or ele-
13 ment of the Department by not later than October
14 1, 2020.

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

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

20 (2) A strategy for mitigating risk to the pro-
21 grams of the Strategic Capabilities Office while the
22 elimination or transfer is carried out.

23 (3) A strategy for implementing the lessons
24 learned and best practices of the Strategic Capabili-

1 ties Office across the organizations and elements of
2 the Department of Defense to promote enterprise-
3 wide innovation.

4 (c) FORM OF PLAN.—The plan required under sub-
5 section (a) shall be submitted in unclassified form, but
6 may include a classified annex.

1 **SEC. 2** **[Log 67406]. EXTENSION OF DIRECTED ENERGY**
2 **PROTOTYPE AUTHORITY.**

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

6 (1) in subparagraph (A), by striking “Except as
7 provided in subparagraph (B)” and inserting “Ex-
8 cept as provided in subparagraph (C)”;

9 (2) by redesignating subparagraph (B) as sub-
10 paragraph (C);

11 (3) by inserting after subparagraph (A) the fol-
12 lowing:

13 “(B) Except as provided in subparagraph (C)
14 and subject to the availability of appropriations for
15 such purpose, of the funds authorized to be appro-
16 priated by the National Defense Authorization Act
17 for Fiscal Year 2019 or otherwise made available for
18 fiscal year 2019 for research, development, test, and
19 evaluation, defense-wide, up to \$100,000,000 may be
20 available to the Under Secretary to allocate to the
21 military departments, the defense agencies, and the
22 combatant commands to carry out the program es-
23 tablished under paragraph (1).”; and

1 (4) in subparagraph (C), as so redesignated, by
2 striking “made available under subparagraph (A)”
3 and inserting “made available under subparagraph
4 (A) or subparagraph (B)”.

1 **SEC. 2** **[Log 67407]. MODIFICATION OF AUTHORITY TO**
2 **CARRY OUT CERTAIN PROTOTYPE PROJECTS.**

3 Section 2371b(f) of title 10, United States Code, is
4 amended by adding at the end the following new para-
5 graphs:

6 “(4) Contracts or transactions entered into pursuant
7 to this subsection that are expected to cost the Depart-
8 ment of Defense in excess of \$100,000,000 but not in ex-
9 cess of \$500,000,000 (including all options) may be
10 awarded only upon written determination by the senior
11 procurement executive for the agency as designated for the
12 purpose of section 1702(c) of title 41, or, by the senior
13 procurement executive for the Defense Advanced Research
14 Projects Agency or the Missile Defense Agency that award
15 of the contract or transaction is essential to meet critical
16 national security interests.

17 “(5) Contracts and transactions entered into pursu-
18 ant to this subsection that are expected to cost the Depart-
19 ment of Defense in excess of \$500,000,000 (including all
20 options) may be awarded only if—

21 “(A) the Under Secretary of Defense for Acqui-
22 sition and Sustainment determines in writing that
23 award of the contract or transaction is essential to
24 meet critical national security objectives; and

1 “(B) the congressional defense committees are
2 notified in writing not later than 30 days before
3 award of the contract or transaction.”.

1 **SEC. 2** **[Log 67739]. LIMITATION ON AVAILABILITY OF**
2 **FUNDS FOR CERTAIN HIGH ENERGY LASER**
3 **ADVANCED TECHNOLOGY.**

4 (a) **LIMITATION.**—Of the funds authorized to be ap-
5 propriated by this Act or otherwise made available for fis-
6 cal year 2019 for the Department of Defense for High
7 Energy Laser Advanced Technology (PE 0603924D8Z),
8 not more than 50 percent may be obligated or expended
9 until the date on which the Secretary of Defense submits
10 to the congressional defense committees—

11 (1) a logical roadmap and detailed assessment
12 of the high energy laser programs of the Depart-
13 ment of Defense; and

14 (2) a justification for the \$33,533,000 of in-
15 creased funding for high energy laser programs au-
16 thORIZED in the National Defense Authorization Act
17 for Fiscal Year 2018 (Public Law 115–91).

18 (b) **RULE OF CONSTRUCTION.**—The limitation in
19 subsection (a) shall not be construed to apply to any other
20 high energy laser program of the Department of Defense
21 other than the program element specified in such sub-
22 section.

1 **SEC. 2** **[Log 67300]. BRIEFING ON USE OF QUANTUM**
2 **SCIENCES FOR MILITARY APPLICATIONS AND**
3 **OTHER PURPOSES.**

4 (a) **BRIEFING REQUIRED.**—Not later than 180 days
5 after the date of the enactment of this Act, the Secretary
6 of Defense shall provide to the congressional defense com-
7 mittees a briefing on the strategy of the Secretary for
8 using quantum sciences for military applications and other
9 purposes.

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

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

16 (2) a plan that describes how the Secretary in-
17 tends to use quantum sciences for military applica-
18 tions and to meet other needs of the Department;
19 and

20 (3) an assessment of the efforts of foreign pow-
21 ers to use quantum sciences for military applications
22 and other purposes.

1 (c) FORM OF BRIEFING.—The briefing under sub-
2 section (a) may be provided in classified or unclassified
3 form.

1 **SEC. 5** **[log 67363]. ENHANCEMENT AND CLARIFICATION**
2 **OF FAMILY SUPPORT SERVICES FOR FAMILY**
3 **MEMBERS OF MEMBERS OF SPECIAL OPER-**
4 **ATIONS FORCES.**

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

7 (1) by striking “activities” each place it appears
8 and inserting “services”;

9 (2) in subsection (b)(2), by striking “activity”
10 and inserting “service”;

11 (3) in subsection (c), by striking “\$5,000,000”
12 and inserting “\$10,000,000”;

13 (4) in subsection (d)(1), by striking “there-
14 after” and inserting “of the next two years”; and

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

17 “(4) The term ‘family support services’ includes
18 costs of transportation, food, lodging, child care,
19 supplies, fees, and training materials for immediate
20 family members of members of the armed forces as-
21 signed to special operations forces while partici-
22 pating in programs under subsection (a).”.

1 **SEC. 8** [Log 67336]. **CONSOLIDATED BUDGET JUSTIFICA-**
2 **TION FOR THE DEPARTMENT OF DEFENSE**
3 **SMALL BUSINESS INNOVATION RESEARCH**
4 **PROGRAM AND SMALL BUSINESS TECH-**
5 **NOLOGY TRANSFER PROGRAM.**

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

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

21 (1) the amount obligated or expended, by ap-
22 propriation and functional area, for each activity
23 conducted under a Small Business Innovation Re-
24 search Program or Small Business Technology

1 Transfer Program, with supporting narrative de-
2 scriptions and rationale for the funding levels; and

3 (2) a summary and estimate of funding re-
4 quired during the period covered by the current fu-
5 ture-years defense program (as defined under section
6 221 of title 10, United States Code).

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

1 **SEC. 9** [Log 67294]. **ARTIFICIAL INTELLIGENCE AND MA-**
2 **CHINE LEARNING POLICY AND OVERSIGHT**
3 **COUNCIL.**

4 (a) **ESTABLISHMENT.**—In order to fulfill the respon-
5 sibilities specified in Section 133a of title 10, United
6 States Code, the Under Secretary of Defense for Research
7 and Engineering shall establish and lead a team to be
8 known as the “Artificial Intelligence and Machine Learn-
9 ing Policy and Oversight Council” (in this section referred
10 to as the “Council”).

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

13 (1) integrate the functional activities of the or-
14 ganizations and elements of the Department of De-
15 fense with respect to artificial intelligence and ma-
16 chine learning;

17 (2) ensure there are efficient and effective arti-
18 ficial intelligence and machine learning capabilities
19 throughout Department; and

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

1 ligence and machine learning throughout the De-
2 partment.

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

5 (1) The Under Secretary of Defense for Re-
6 search and Engineering, or the designee of the
7 Under Secretary, who shall serve as the leader of the
8 Council.

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

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

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

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

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

19 (E) The Under Secretary of Defense for
20 Intelligence.

21 (F) The General Counsel of the Depart-
22 ment of Defense.

23 (G) The head of each military service.

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

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

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

6 (d) OPERATION.—The Council shall operate continu-
7 ously.

1 **SEC. 10** [Log 67283]. **DEFINITION OF SENSITIVE MILITARY**
2 **OPERATION.**

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

5 “(d) **SENSITIVE MILITARY OPERATION DEFINED.**—

6 (1) Except as provided in paragraph (2), in this section,
7 the term ‘sensitive military operation’ means a lethal oper-
8 ation or capture operation conducted by the armed forces
9 or conducted by a foreign partner in coordination with the
10 armed forces that targets a specific individual or individ-
11 uals.

12 “(2) For purposes of this section, the term ‘sensitive
13 military operation’ does not include any operation con-
14 ducted within Afghanistan.”.

1 **SEC. 10** [Log 67295]. **DEPARTMENT OF DEFENSE REVIEW**
2 **AND ASSESSMENT ON ADVANCES IN ARTIFI-**
3 **CIAL INTELLIGENCE AND MACHINE LEARN-**
4 **ING.**

5 (a) **REVIEW REQUIRED.**—The Secretary of Defense,
6 acting through the Defense Innovation Board and the
7 Under Secretary of Defense for Research and Engineer-
8 ing, shall carry out a review and assessment of the ad-
9 vances in artificial intelligence, related machine learning
10 developments, and associated technologies for military ap-
11 plications. In carrying out such review, the Secretary shall
12 consider the methods and means necessary to advance the
13 development of artificial intelligence, machine learning,
14 and associated technologies within the Department of De-
15 fense to comprehensively address the national security
16 needs and requirements of the Department of Defense.

17 (b) **SCOPE OF REVIEW.**—In conducting the review
18 under paragraph (a) the Secretary of Defense shall con-
19 sider—

20 (1) the competitiveness of the Department of
21 Defense in artificial intelligence, machine learning,
22 and other associated technologies, including matters
23 pertaining to public-private partnerships and invest-
24 ments;

1 (2) means and methods for the Department of
2 Defense to maintain a technological advantage in ar-
3 tificial intelligence, machine learning, and other as-
4 sociated technologies, including quantum sciences
5 and high performance computing;

6 (3) means by which the Department of Defense
7 can help foster greater emphasis and investments in
8 basic and advanced research to stimulate private,
9 public, academic, and combined initiatives in artifi-
10 cial intelligence, machine learning, and other associ-
11 ated technologies, including quantum sciences, and
12 high performance computing;

13 (4) Department of Defense workforce and edu-
14 cation initiatives to attract and recruit leading talent
15 in artificial intelligence and machine learning, in-
16 cluding science, technology, engineering, and math
17 programs;

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

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

25 (c) REPORTS.—

1 (1) INITIAL REPORT.—Not later than 180 days
2 after the date of the enactment of this Act, the Sec-
3 retary of Defense shall submit to the congressional
4 defense committees an initial report on the findings
5 of the review required under subsection (a) and such
6 recommendations as the Secretary may have for leg-
7 islative action related to artificial intelligence, ma-
8 chine learning, and associated technologies, includ-
9 ing recommendations to more effectively fund and
10 organize the Department of Defense.

11 (2) COMPREHENSIVE REPORT.—Not later than
12 one year after the date of the enactment of this Act,
13 the Secretary of Defense shall submit to the con-
14 gressional defense committees a comprehensive re-
15 port on the review required under subsection (a).

16 (d) DEFINITION OF ARTIFICIAL INTELLIGENCE.—In
17 this section, the term “artificial intelligence” includes each
18 of the following:

19 (1) Any artificial system that performs tasks
20 under varying and unpredictable circumstances with-
21 out significant human oversight, or that can learn
22 from experience and improve performance when ex-
23 posed to data sets.

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

1 solves tasks requiring human-like perception, cog-
2 nition, planning, learning, communication, or phys-
3 ical action.

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

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

10 (5) An artificial system designed to act ration-
11 ally, including an intelligent software agent or em-
12 bodied robot that achieves goals using perception,
13 planning, reasoning, learning, communicating, deci-
14 sionmaking, and acting.

1 **SEC. 10** [Log 67499]. **REPORT ON PROPOSED CONSOLIDA-**
2 **TION OF DEPARTMENT OF DEFENSE GLOBAL**
3 **MESSAGING AND COUNTER MESSAGING CA-**
4 **PABILITIES.**

5 (a) **REPORT REQUIRED.**—The Secretary of Defense
6 shall submit to the congressional defense committees a re-
7 port on the proposed consolidation of the global messaging
8 and counter messaging (GMCM) capabilities of the De-
9 partment of Defense. Such report shall include each of the
10 following:

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

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

17 (3) A description of the proposed roles and re-
18 sponsibilities of the United States Special Oper-
19 ations Command as such entity.

20 (4) A description of the roles and responsibil-
21 ities of the combatant commanders regarding the
22 operational use of the GMCM capability.

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

4 (6) An implementation plan that includes a de-
5 tailed description of the resources and other require-
6 ments required for the United States Special Oper-
7 ations Command to establish the centralized GMCM
8 capability for the period covered by the current fu-
9 ture year's defense program.

10 (7) A comprehensive plan for the continual as-
11 sessment of the effectiveness of the GMCM activities
12 and programs.

13 (8) An identification of the anticipated effi-
14 ciencies, cost savings, and operational benefits asso-
15 ciated with the consolidation of the GMCM capabili-
16 ties.

17 (9) A description of any actions, activities, and
18 efforts taken to implement section 1637 of the Na-
19 tional Defense Authorization Act for Fiscal Year
20 2018 (Public Law 115–91).

21 (b) LIMITATION ON USE OF FUNDS.—Not more than
22 50 percent of the amounts authorized to be appropriated
23 by this Act or otherwise made available for fiscal year
24 2019 for the Commander of the United States Special Op-
25 erations Command for global messaging and counter mes-

- 1 saging may be obligated or expended before the date that
- 2 is 30 days after the date on which the Secretary submits
- 3 the report required by subsection (a).

1 **SEC. 10** ___ [Log 67535]. **PRINCIPAL ADVISOR ON COUN-**
2 **TERING WEAPONS OF MASS DESTRUCTION.**

3 (a) IN GENERAL.—

4 (1) DESIGNATION OF PRINCIPAL ADVISOR.—

5 Chapter 4 of title 10, United States Code, is amend-
6 ed by adding at the end the following new section:

7 **“§ 145. Principal Advisor on Countering Weapons of**
8 **Mass Destruction**

9 “(a) DESIGNATION.—The Secretary of Defense shall
10 designate, from among the personnel of the Office of the
11 Secretary of Defense, a Principal Advisor on Countering
12 Weapons of Mass Destruction. Such Principal Advisor
13 shall act as the principal advisor to the Secretary on the
14 activities of the Department of Defense relating to coun-
15 tering weapons of mass destruction. The individual des-
16 igned to serve as such Principal Advisor shall be an indi-
17 vidual who was appointed to the position held by the indi-
18 vidual by and with the advice and consent of the Senate.

19 “(b) RESPONSIBILITIES.—The Principal Advisor des-
20 igned under subsection (a) shall carry out the following
21 responsibilities:

22 “(1) Supervising the activities of the Depart-
23 ment of Defense relating to countering weapons of
24 mass destruction, including the oversight of policy

1 and operational considerations, resources, personnel,
2 acquisition, and technology.

3 “(2) Carrying out such other responsibilities re-
4 lating to countering weapons of mass destruction as
5 the Secretary shall specify.”.

6 (2) CLERICAL AMENDMENT.—The table of sec-
7 tions at the beginning of such chapter is amended
8 by adding at the end the following new item:

“145. Principal Advisor on Countering Weapons of Mass Destruction.”.

9 (b) OVERSIGHT PLAN.—Not later than 180 days
10 after the date of the enactment of this Act, the Secretary
11 of Defense shall submit to the congressional defense com-
12 mittees a plan to streamline the oversight framework of
13 the Office of the Secretary of Defense, including any effi-
14 ciencies and the potential to reduce, realign, or otherwise
15 restructure current Assistant Secretary and Deputy As-
16 sistant Secretary positions with responsibilities for over-
17 seeing countering weapons of mass destruction policy, pro-
18 grams, and activities.

1 **SEC. 10** [Log 67622]. **COMPREHENSIVE REVIEW OF PRO-**
2 **FESSIONALISM AND ETHICS PROGRAMS FOR**
3 **SPECIAL OPERATIONS FORCES.**

4 (a) **REVIEW REQUIRED.**—The Secretary of Defense,
5 in coordination with the Secretaries of each of the military
6 departments, shall conduct a comprehensive review of the
7 ethics and professionalism programs of the United States
8 Special Operations Command and of the military depart-
9 ments for officers and other military personnel serving in
10 special operations forces.

11 (b) **ELEMENTS OF THE REVIEW.**—The review con-
12 ducted under subsection (a) shall specifically include a de-
13 scription and assessment of each of the following:

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

17 (2) The ethics and professionalism programs of
18 the military departments available for special oper-
19 ations forces.

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

23 (4) The roles and responsibilities of the military
24 departments and the United States Special Oper-

1 ations Command and affiliated component com-
2 mands in administering, overseeing, managing, and
3 ensuring compliance and participation of special op-
4 erations forces in ethics and professionalism pro-
5 grams, including an identification of—

6 (A) gaps in the administration, oversight,
7 and management of such programs and in en-
8 suring the compliance and participation in such
9 programs; and

10 (B) additional guidance that may be re-
11 quired for a systematic, integrated approach in
12 administering, overseeing, and managing such
13 programs and in ensuring compliance with and
14 participation in such programs in order to ad-
15 dress issues and improve ethical culture and
16 professionalism.

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

21 (6) Tools and metrics for identifying and as-
22 sassing individual and organizational ethics and pro-
23 fessionalism issues with respect to special operations
24 forces.

1 (7) Tools and metrics for assessing the effec-
2 tiveness of existing ethics and professionalism pro-
3 grams in improving or addressing individual and or-
4 ganizational ethics-related and professionalism issues
5 with respect to special operations forces.

6 (8) Additional programs or actions that may be
7 required to address or improve individual and orga-
8 nizational ethics and professionalism issues with re-
9 spect to special operations forces.

10 (9) Actions to improve the oversight and ac-
11 countability by senior leaders of ethics and profes-
12 sionalism-related issues with respect to special oper-
13 ations forces.

14 (c) DEFINITIONS.—In this section:

15 (1) The term “ethics program” means a pro-
16 gram that includes—

17 (A) compliance-based ethics training, edu-
18 cation, initiative, or other activity that focuses
19 on adherence to rules and regulations; and

20 (B) values-based ethics training, education,
21 initiative, or other activity that focuses on up-
22 holding a set of ethical principles in order to
23 achieve high standards of conduct and incor-
24 porate guiding principles to help foster an eth-

1 ical culture and inform decision-making where
2 rules are not clear.

3 (2) The term “professionalism program” means
4 a program that includes training, education, initia-
5 tive, or other activity that focuses on values, ethics,
6 standards, code of conduct, and skills as related to
7 the military profession.

8 (d) SUBMITTAL OF REVIEW.—The Secretary of De-
9 fense shall submit the review required by subsection (a)
10 to the Committees on Armed Services of the Senate and
11 the House of Representatives by not later than March 1,
12 2019.

1 **SEC. 12__.** **[LOG 67774] THREE-YEAR EXTENSION OF AU-**
2 **THORIZATION OF NON-CONVENTIONAL AS-**
3 **SISTED RECOVERY CAPABILITIES.**

4 Section 943(g) of the National Defense Authorization
5 Act for Fiscal Year 2009 (Public Law 110–417; 122 Stat.
6 4579), as most recently amended by section 1051(n) of
7 the National Defense Authorization Act for Fiscal Year
8 2018 (Public Law 115–91; 131 Stat. 1564), is further
9 amended by striking “2021” and inserting “2024”.

1 **SEC. 12___.** **[LOG 67550] UNITED STATES-ISRAEL COUN-**
2 **TERING UNMANNED AERIAL SYSTEMS CO-**
3 **OPERATION.**

4 Section 1279(a) of the National Defense Authoriza-
5 tion Act for Fiscal Year 2016 (Public Law 114–92; 22
6 U.S.C. 8606 note), as most recently amended by section
7 1278 of the National Defense Authorization Act for Fiscal
8 Year 2018 (Public Law 115–91; 131 Stat. 1700), is fur-
9 ther amended—

10 (1) by inserting “and capabilities for countering
11 unmanned aerial systems” after “anti-tunnel capa-
12 bilities”; and

13 (2) by inserting “and unmanned aerial sys-
14 tems” after “underground tunnels”.

1 **SEC. 12__.** **[LOG 67298] NATO COOPERATIVE CYBER DE-**
2 **FENSE CENTER OF EXCELLENCE.**

3 (a) **AUTHORIZATION.**—The Secretary of Defense
4 shall provide funds for the NATO Cooperative Cyber De-
5 fense Center of Excellence (in this section referred to as
6 the “Center”) to—

7 (1) enhance the ability of military forces and ci-
8 vilian personnel of the countries participating in the
9 Center to engage in joint cyber exercises or coalition
10 or international military operations; and

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

14 (b) **CERTIFICATION.**—Not later than 180 days after
15 the date of the enactment of this Act, the Secretary of
16 Defense shall certify to the Committees on Armed Services
17 of the House of Representatives and the Senate that the
18 Secretary has assigned executive agent responsibilities for
19 the Center to an appropriate organization within the De-
20 partment of Defense, and detail the steps being under-
21 taken to strengthen the role of the Center in fostering
22 cyber defense and cyber warfare capabilities within
23 NATO.

1 (c) BRIEFING REQUIREMENT.—The Secretary of De-
2 fense shall periodically brief the Committee on Armed
3 Services and the Committee on Foreign Relations of the
4 Senate and the Committee on Armed Services and the
5 Committee on Foreign Affairs of the House of Representa-
6 tives on the efforts of the Department of Defense to
7 strengthen the role of the Center in fostering cyber de-
8 fense and cyber warfare capabilities within NATO.

1 **SEC. 12__ . [LOG 67299] NATO STRATEGIC COMMUNICATIONS**

2 **CENTER OF EXCELLENCE.**

3 (a) AUTHORIZATION.—The Secretary of Defense
4 shall provide funds for the NATO Strategic Communica-
5 tions Center of Excellence (in this section referred to as
6 the “Center”) to—

7 (1) enhance the ability of military forces and ci-
8 vilian personnel of the countries participating in the
9 Center to engage in joint strategic communications
10 exercises or coalition or international military oper-
11 ations; and

12 (2) improve interoperability between the armed
13 forces and the military forces of friendly foreign na-
14 tions in the areas of strategic communications.

15 (b) CERTIFICATION.—Not later than 180 days after
16 the date of the enactment of this Act, the Secretary of
17 Defense shall certify to the Committees on Armed Services
18 of the House of Representatives and the Senate that the
19 Secretary has assigned executive agent responsibility for
20 the Center to an appropriate organization within the De-
21 partment of Defense, and detail the steps being under-
22 taken to strengthen the role of the Center in fostering
23 strategic communications and information operations
24 within NATO.

1 (c) BRIEFING REQUIREMENT.—The Secretary of De-
2 fense shall periodically brief the Committee on Armed
3 Services and the Committee on Foreign Relations of the
4 Senate and the Committee on Armed Services and the
5 Committee on Foreign Affairs of the House of Representa-
6 tives on the efforts of the Department of Defense to
7 strengthen the role of the Center in fostering strategic
8 communications and information operations within
9 NATO.

1 **SEC. 13** ____ **[Log 67547]. FUNDING ALLOCATIONS.**

2 Of the \$335,240,000 authorized to be appropriated
3 to the Department of Defense for fiscal year 2019 in sec-
4 tion 301 and made available by the funding table in divi-
5 sion D for the Department of Defense Cooperative Threat
6 Reduction Program established under section 1321 of the
7 Department of Defense Cooperative Threat Reduction Act
8 (50 U.S.C. 3711), the following amounts may be obligated
9 for the purposes specified:

10 (1) For strategic offensive arms elimination,
11 \$2,823,000.

12 (2) For chemical weapons destruction,
13 \$5,446,000.

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

15 (4) For cooperative biological engagement,
16 \$197,585,000.

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

18 (6) For activities designated as Other Assess-
19 ments/Administrative Costs, \$25,448,000.

1 **SEC. 13** **[Log 67548]. SPECIFICATION OF COOPERATIVE**
2 **THREAT REDUCTION FUNDS.**

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

1 **SEC. 14** ____ . **[LOG 67212] QUARTERLY BRIEFING ON**
2 **PROGRESS OF CHEMICAL DEMILITARIZATION**
3 **PROGRAM.**

4 Section 1412(j) of the Department of Defense Au-
5 thorization Act, 1986 (50 U.S.C. 1521(j)) is amended—

6 (1) in the heading, by striking “Semiannual Re-
7 ports” and inserting “QUARTERLY BRIEFING”;

8 (2) in paragraph (1)—

9 (A) by striking “March 1” and all that fol-
10 lows through “the year in which” and inserting
11 “90 days after the date of the enactment of the
12 National Defense Authorization Act for Fiscal
13 Year 2019, and every 90 days thereafter until”;

14 (B) by striking “submit to” and inserting
15 “brief”;

16 (C) by striking “a report on the implemen-
17 tation” and inserting “on the progress made”;
18 and

19 (D) by striking “of its chemical weapons
20 destruction obligations” and inserting “toward
21 fulfilling its chemical weapons destruction obli-
22 gations”; and

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

1 “(2) Each briefing under paragraph (1) shall
2 include a description of contractor costs and per-
3 formance relative to schedule, the progress to date
4 toward the complete destruction of the stockpile, and
5 any other information the Secretary determines to
6 be relevant.”.

1 **SEC. 16** **[Log 67302]. STUDY AND REPORT ON RESERVE**
2 **COMPONENT CYBER CIVIL SUPPORT TEAMS.**

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

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

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

14 (2) An analysis of State and local civilian and
15 private sector cyber response capabilities and serv-
16 ices, including an identification of any gaps in such
17 capabilities and services.

18 (3) An identification of the potential role of
19 such teams with respect to the principles and proc-
20 esses set forth in—

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

23 (B) Presidential Policy Directive 21 (Crit-
24 ical Infrastructure Security and Resilience); and

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

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

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

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

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

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

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

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

1 (B) to perform civilian cyber response mis-
2 sions.

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

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

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

12 (1) the results of the study conducted under
13 subsection (a), including an explanation of each ele-
14 ment described in subsection (b);

15 (2) the final determination of the Secretaries
16 with respect to the feasibility, advisability, and ne-
17 cessity of establishing reserve component cyber civil
18 support teams for each State; and

19 (3) if such final determination is in the affirma-
20 tive, proposed legislation for the establishment of the
21 teams, which may include proposed legislation to
22 amend section 12310 of title 10, United States
23 Code.

24 (d) DEFINITIONS.—In this section:

1 (1) The term “appropriate congressional com-
2 mittees” means—

3 (A) the congressional defense committees;

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

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

8 (2) The term “reserve component cyber civil
9 support team” means a team that—

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

12 (B) is organized, trained, equipped, and
13 sustained by the Department of Defense for the
14 purpose of assisting State authorities in pre-
15 paring for and responding to cyber incidents,
16 cyber emergencies, and cyber attacks; and

17 (C) operates principally under the com-
18 mand and control of the Chief Executive of the
19 State in which the team is located.

20 (3) The term “Secretaries concerned” means
21 the Secretary of Defense and the Secretary of
22 Homeland Security acting jointly.

23 (4) The term “State” means each of the several
24 States, the District of Columbia, the Commonwealth

1 of Puerto Rico, and the United States Virgin Is-
2 lands.

1 **SEC. 16 ____ . [Log 67332] PILOT PROGRAM AUTHORITY TO**
2 **ENHANCE CYBERSECURITY AND RESILIENCY**
3 **OF CRITICAL INFRASTRUCTURE.**

4 (a) **AUTHORITY.**—The Secretary of Defense, in co-
5 ordination with the Secretary of Homeland Security, is au-
6 thorized to provide, detail, or assign technical personnel
7 to the Department of Homeland Security on a non-reim-
8 bursable basis to enhance cybersecurity cooperation, col-
9 laboration, and unity of Government efforts.

10 (b) **SCOPE OF ASSISTANCE.**—The authority under
11 subsection (a) shall be limited in any fiscal year to the
12 provision of not more than 50 technical cybersecurity per-
13 sonnel from the Department of Defense to the Depart-
14 ment of Homeland Security, including the national cyber-
15 security and communications integration center (NCCIC)
16 of the Department, or other locations as agreed upon by
17 the Secretary of Defense and the Secretary of Homeland
18 Security.

19 (c) **LIMITATION.**—The authority under subsection (a)
20 may not negatively impact the primary missions of the De-
21 partment of Defense or the Department of Homeland Se-
22 curity.

23 (d) **ESTABLISHMENT OF PROCEDURES.**—

1 (1) IN GENERAL.—The Secretary of Defense
2 and the Secretary of Homeland Security shall estab-
3 lish procedures to carry out subsection (a), including
4 procedures relating to the protection of and safe-
5 guards for maintenance of information held by the
6 NCCIC regarding United States persons.

7 (2) LIMITATION.—Nothing in this subsection
8 may be construed as providing authority to the Sec-
9 retary of Defense to establish procedures regarding
10 the NCCIC with respect to any matter outside the
11 scope of this section.

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

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

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

1 **SEC. 16** ____ . **[Log 67333] PROCEDURES AND REPORTING RE-**
2 **QUIREMENT ON CYBERSECURITY BREACHES**
3 **AND LOSS OF PERSONALLY IDENTIFIABLE IN-**
4 **FORMATION.**

5 (a) **IN GENERAL.**—In the event of a significant loss
6 of personally identifiable information of civilian or uni-
7 formed members of the Armed Forces, the Secretary of
8 Defense shall promptly submit to the congressional de-
9 fense committees notice in writing of such loss. Such no-
10 tice may be submitted in classified or unclassified formats.

11 (b) **PROCEDURES.**—Not later than 180 days after the
12 date of the enactment of this Act, the Secretary of Defense
13 shall establish and submit to the congressional defense
14 committees procedures for complying with the require-
15 ments of subsection (a). Such procedures shall be con-
16 sistent with the national security of the United States, the
17 protection of operational integrity, and the protection of
18 personally identifiable information of civilian and uni-
19 formed members of the Armed Forces.

20 (c) **SIGNIFICANT LOSS OF PERSONALLY IDENTIFI-**
21 **ABLE INFORMATION DEFINED.**—In this section, the term
22 “significant loss of personally identifiable information”
23 means an intentional, accidental, or otherwise known dis-
24 closure of information that can be used to distinguish or

1 trace an individual's identity, such as the name, social se-
2 curity number, date and place of birth, biometric records,
3 home or other phone numbers, or other demographic, per-
4 sonnel, medical, or financial information, involving 250 or
5 more civilian or uniformed members of the Armed Forces.

1 **SEC. 16____. [Log 67337] AMENDMENTS TO PILOT PROGRAM**
2 **REGARDING CYBER VULNERABILITIES OF**
3 **DEPARTMENT OF DEFENSE CRITICAL INFRA-**
4 **STRUCTURE.**

5 Subsection (b) of section 1650 of the National De-
6 fense Authorization Act for Fiscal Year 2017 (10 U.S.C.
7 2224 note) is amended—

8 (1) in paragraph (1), in the matter preceding
9 subparagraph (A), by inserting “and the Defense
10 Digital Service” after “covered research laboratory”;

11 (2) in paragraph (4), in the matter preceding
12 subparagraph (A), by striking “2019” and inserting
13 “2020”; and

14 (3) in paragraph (5), by striking “2019” and
15 inserting “2020”.

1 **SEC. 16 ____.** **[Log 67358]** **TRANSFER OF RESPONSIBILITY**
2 **FOR THE DEPARTMENT OF DEFENSE INFOR-**
3 **MATION NETWORK TO UNITED STATES**
4 **CYBER COMMAND.**

5 (a) **IN GENERAL.**—Not later than September 30,
6 2019, the Secretary of Defense shall transfer all roles,
7 missions, and responsibilities of the Commander, Joint
8 Force Headquarters - Department of Defense Information
9 Networks (JFHQ-DODIN) from the Defense Information
10 Support Agency to the Commander, United States Cyber
11 Command.

12 (b) **CERTIFICATION REQUIRED.**—Prior to the trans-
13 fer required under subsection (a), the Secretary of De-
14 fense shall certify in writing to the congressional defense
15 committees that such transfer shall not result in mission
16 degradation.

1 **SEC. 16____. [Log 67647] BUDGET DISPLAY FOR CYBER VUL-**
2 **NERABILITY EVALUATIONS AND MITIGATION**
3 **ACTIVITIES FOR MAJOR WEAPON SYSTEMS**
4 **OF THE DEPARTMENT OF DEFENSE.**

5 (a) BUDGET REQUIRED.—Beginning in fiscal year
6 2021 and in each fiscal year thereafter, the Secretary of
7 Defense shall submit to Congress, as a part of the docu-
8 mentation that supports the President’s annual budget for
9 the Department of Defense, a consolidated Cyber Vulner-
10 ability Evaluation and Mitigation budget justification dis-
11 play for each major weapons system of the Department
12 of Defense that includes the following:

13 (1) CYBER VULNERABILITY EVALUATIONS.—

14 (A) STATUS.—Whether, in accordance with
15 paragraph (1) of section 1647(a) of the Na-
16 tional Defense Authorization Act for Fiscal
17 Year 2016 (Public Law 114–92; 129 Stat.
18 1118), the cyber vulnerability evaluation for
19 each such major weapon system is pending, in
20 progress, complete, or, pursuant to paragraph
21 (2) of such section, waived.

22 (B) FUNDING.—The funding required for
23 the fiscal year with respect to which the budget
24 is submitted and for at least the four suc-

1 ceeding fiscal years required to complete the
2 pending or in progress cyber vulnerability eval-
3 uation of each such major weapon system.

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

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

15 (2) MITIGATION ACTIVITIES.—

16 (A) STATUS.—Whether activities to ad-
17 dress identified cyber vulnerabilities of such
18 major weapon systems resulting in operational
19 or security risks requiring mitigation are pend-
20 ing, in progress, or complete.

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

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

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

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

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

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

Items of Special Interest

Counter-unmanned aerial system threat detection

Future uses of synthetic biology

Innovative installation capabilities

Military Free Fall School

National Hypersonics Initiative

National lab integration in defense innovation hubs

TITLE V—MILITARY PERSONNEL POLICY

ITEMS OF SPECIAL INTEREST

U.S. Special Operations Command Preservation of the Force and Families

Program Contract Support

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

Civil Support Team Information Management System

Counterterrorism Effectiveness Research

Genetic and Medical Information Security

MQ-9 Enterprise Supporting Air Combat Command and Air Force Special

Operations Command Activities

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

TITLE XIII—COOPERATIVE THREAT REDUCTION

ITEMS OF SPECIAL INTEREST

Future of the Cooperative Threat Reduction Program

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND

INTELLIGENCE MATTERS

ITEMS OF SPECIAL INTEREST

CYBER-RELATED MATTERS

Comptroller General Review of Current Military Cyber Operations

Comptroller General Review of Information Operations Strategy

INTELLIGENCE MATTERS

Insider Threat Detection and User Activity Monitoring

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 coordination 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.