H.R. 2810—FY18 NATIONAL DEFENSE AUTHORIZATION BILL

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

SUMMARY OF BILL LANGUAGE

Table Of Contents

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

LEGISLATIVE PROVISIONS

SUBTITLE B—PROGRAM REQUIREMENTS, RESTRICTIONS, AND LIMITATIONS

Section 2XX—Modification of Authority to Award Prizes for Advanced Technology Achievements

This section would amend section 2374a of title 10, United States Code, to make permanent the Secretary of Defense's authority to award prizes for advanced technology achievements, to allow for the award of non-monetary awards, and to authorize the acceptance of non-monetary items from other parts of the Federal Government, from State government, and from non-governmental sources.

Section 2XX—Capital Investment Authority

This section would amend section 2208(k)(2) of title 10, United States Code, to raise the limit on capital purchases from defense working capital funds from $0.25 million to $0.5 million.

Section 2XX—Hypersonic Airbreathing Weapons Capabilities

This section would allow the Secretary of Defense to transfer oversight and management of the Hypersonic Airbreathing Weapons Concept from the Defense Advanced Research Projects Agency to an entity of the Air Force.

Section 2XX—Joint Hypersonics Transition Office

This section would re-designate the "Joint Technology Office on Hypersonics" as the "Joint Hypersonics Transition Office," with the responsibility to coordinate and integrate programs, ensure coordination of current and future programs of the Department of Defense on hypersonics, and approve demonstrations.

TITLE V—MILITARY PERSONNEL POLICY

LEGISLATIVE PROVISIONS

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

Section 5XX—Codification of Authority to Conduct Family Support Programs for Immediate Family Members of Members of the Armed Forces Assigned to Special Operations Forces

This section would make permanent the authority provided by section 554 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66), as modified by section 574(a) of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92) by adding a new section to chapter 88 of title 10, United States Code. The section would provide the Commander, U.S. Special Operations Command the authority to conduct programs for immediate family members of members of the Armed Forces assigned to special operations forces.

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

LEGISLATIVE PROVISIONS

SUBTITLE A—AMENDMENTS TO GENERAL CONTRACTING AUTHORITIES, PROCEDURES, AND LIMITATIONS

Section 8XX—Clarification to Other Transaction Authority

This section would modify section 2371b of title 10, United States Code, related to other transactions authority (OTA) to ensure consistency across the language and improve clarity for how the Department of Defense makes determinations when higher level authority is needed to sign off on a specific OTA award. The committee believes such changes will improve the speed and efficiency of issuing these awards by reducing the numbers of determinations requiring higher level signature. Due to the changes that have been made to this authority in recent years, the committee encourages the Department to revise and, if necessary, reissue guidance on using OTA.

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

LEGISLATIVE PROVISIONS

Section 9XX—Responsibility of the Chief Information Officer of the Department of Defense for Risk Management Activities regarding Supply Chain for Information Technology Systems

This section would amend section 142(b)(1) of title 10, United States Code, by making the Department of Defense Chief Information Officer responsible for

policy, oversight, guidance, and coordination for supply chain risk management activities for the Department's information technology (IT) systems.

The committee remains concerned that the Department of Defense is not adequately postured or resourced to conduct the necessary planning, analysis, and assessment for supply chain risk management of Department of Defense information technology systems. This problem is exacerbated by the globalized nature of both the hardware and software supply chains for IT, and by the reliance of the Department on primarily commercial systems that are the products of the globalized management and supply chain. While the committee is aware that much progress has been made in developing policies and guidance, as well as creating the core of an analytic capability, the committee believes there is more to be done. In addition to rethinking how to address this problem with less manpower, the committee also believes the Department should do more to invest in automated information feeds, including from business and commercial intelligence providers, to fuse with classified information when needed, but also to provide stand-alone products more easily shareable with industry, interagency, and international partners.

TITLE X—GENERAL PROVISIONS

LEGISLATIVE PROVISIONS

SUBTITLE C—COUNTERTERRORISM

Section 10XX—Termination of Requirement to Submit Annual Budget Justification Display for Department of Defense Combating Terrorism Program

This section would terminate the requirement to submit an annual budget justification display for Department of Defense combating terrorism programs under section 229 of title 10, United States Code, by December 31, 2020.

SUBTITLE D—MISCELLANEOUS AUTHORITIES AND LIMITATIONS

Section 10XX—Limitation on Expenditure of Funds for Emergency and Extraordinary Expenses for Intelligence and Counter-Intelligence Activities and Representation Allowances

This section would modify section 127 of title 10, United States Code, to include an additional notification requirement for intelligence and counter-intelligence activities.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

LEGISLATIVE PROVISIONS

SUBTITLE E—OTHER MATTERS

Section 12XX—NATO Cooperative Cyber Defense Center of Excellence

This section would authorize up to $5.0 million for fiscal year 2018 for the purposes of establishing the NATO Cooperative Cyber 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 up to $5.0 million for fiscal year 2018 for the purposes of establishing 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.

TITLE XIII—COOPERATIVE THREAT REDUCTION

LEGISLATIVE PROVISIONS

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 2018, 2019, and 2020.

The committee also notes that section 1303 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328) mandated the expenditure or obligation of semiannual installments of funds available for Cooperative Threat Reduction Activities in the People's Republic of China, and that such semiannual installments should be made in accordance with all applicable laws, to include chapter 39 of title 31, United States Code, also known as the "Prompt Payment Act."

Section 1302—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 $324.6 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 2018.

TITLE XV—AUTHORIZATION OF ADDITIONAL APPROPRIATIONS FOR OVERSEAS CONTINGENCY OPERATIONS

LEGISLATIVE PROVISIONS

SUBTITLE A—AUTHORIZATION OF ADDITIONAL APPROPRIATIONS

Section 15XX—Joint Improvised Explosive Device Defeat Fund

This section would amend section 1532(a) of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92) to extend the use and transfer authority for the Joint Improvised Explosive Device Defeat Fund through fiscal year 2018. This section would also amend section 1532(c) of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112-239) to extend the authority for interdiction of improvised explosive device precursor chemicals to December 31, 2018.

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE B—DEFENSE INTELLIGENCE AND INTELLIGENCE-RELATED ACTIVITIES

Section 16XX—Extension of Authority to Engage in Certain Commercial Activities

This section would amend section 431(a) of title 10, United States Code, to extend the authority to engage in commercial activities as security for intelligence collection activities through December 31, 2023.

Section 16XX—Submission of Audits of Commercial Activity Funds

This section would modify section 432 of title 10, United States Code, for audits to be submitted to the congressional defense committees and the congressional intelligence committees by not later than December 31 of each year.

SUBTITLE C—CYBERSPACE-RELATED MATTERS

Section 16XX—Plan to Increase Cyber and Information Operations, Deterrence, and Defense

This section would direct the Secretary of Defense to develop a plan to increase regional cyber planning and enhance information operations and strategic communication strategies to counter Chinese and North Korean information

warfare, malign influence, and propaganda activities. It would further direct the Secretary to provide a briefing to the congressional defense committees on the plan not later than 180 days after the date of the enactment of this Act.

Section 16XX—Modification to Quarterly Cyber Operations Briefings

This section would amend section 484 of title 10, United States Code, related to quarterly cyber operations briefings by including all of the congressional defense committees in the requirement, as well as increasing the fidelity of the items to be included in each quarterly briefing. In addition, the committee encourages the Department of Defense to also include reporting on the Cybersecurity Scorecard, how measures of resilience may be addressed by this scorecard, and means for measuring or tracking supply chain risk management activities.

Section 16XX—Cyber Scholarship Program

This section would amend chapter 112 of title 10, United States Code, to establish the Department of Defense Cyber Scholarship Program, setting aside 5 percent of the available funding for pursuit of associate degrees in cyber and authorizing $10.0 million in fiscal year 2018 for such scholarships.

The committee is concerned that lack of funding under this program may further aggravate the challenges the Department is experiencing in recruiting and retaining cyber security personnel. The committee believes that providing additional opportunities under the program will be beneficial in continuing to address Department requirements for a qualified cyber workforce. Further, the committee encourages the Department to use the opportunity to educate the public on this program and to focus on institutions with high-quality computer science, engineering, and cyber security programs, including historically black colleges and universities, and minority-serving institutions, as a way to expand the pool of talented applicants.

Section 16XX—Notification Requirements for Sensitive Military Cyber Operations and Cyber Weapons

This section would amend title 10, United States Code, to require the Secretary of Defense to promptly submit in writing to the congressional defense committees notice of any sensitive military cyber operation and notice of the results of the review of any cyber capability that is intended for use as a weapon. This section would also require the Secretary of Defense to establish procedures for providing such notice in a manner consistent with national security of the United States and the protection of operational integrity.

The term "sensitive military cyber operation" would include cyber actions carried out by the Armed Forces and actions intended to cause effects outside a

geographic location where United States forces are involved in hostilities (as that term is used in section 1543 of title 50, United States Code).

This section is not intended to create or alter reporting requirements of any other agency or department of the Department of Defense.

BILL LANGUAGE

SEC. 2___[Log 64956]. MODIFICATION OF AUTHORITY TO AWARD PRIZES FOR ADVANCED TECHNOLOGY ACHIEVEMENTS.

Section 2374a of title 10, United States Code, is amended—

(1) in subsection (a), by striking ''to award cash prizes'' and inserting ''to award prizes, which may be cash prizes or nonmonetary prizes,'';

(2) in subsection (b), by striking ''cash prizes'' and inserting ''prizes'';

(3) in subsection (c)—

(A) in paragraph (1), by striking ''cash prize of'' and inserting ''prize valued at''; and

(B) by adding at the end the following:

''(3) No prize competition may result in the award of a nonmonetary prize valued at more than $10,000 without the approval of the Under Secretary of Defense for Acquisition, Technology, and Logistics.'';

(4) in subsection (e)—

(A) by inserting ''or nonmonetary items'' after ''accept funds''; and

(B) by striking ''and from State and local governments,'' and inserting ''from State and

local governments, and from other nongovernmental sources,''; and

(5) by striking subsection (f).

SEC. 2___[Log 65383]. CAPITAL INVESTMENT AUTHORITY.

Section 2208(k)(2) of title 10, United States Code, is amended by striking ''$250,000'' and inserting ''$500,000''.

SEC. 2___[Log 65537]. HYPERSONIC AIRBREATHING WEAPONS CAPABILITIES.

(a) IN GENERAL.—The Secretary of Defense may transfer oversight and management of the Hypersonic Airbreathing Weapons Concept from the Defense Advanced Research Projects Agency to a responsible entity of the Air Force. The Secretary of the Air Force, acting through the head of the Air Force Research Laboratory, shall continue—

(1) to develop a reusable hypersonics test bed to further probe the high speed flight corridor and to facilitate the testing and development of hypersonic airbreathing weapon systems;

(2) to explore emerging concepts and technologies for reusable hypersonics weapons systems beyond current hypersonics programs, focused on experimental flight test capabilities; and

(3) to develop defensive technologies and countermeasures against potential and identified hypersonic threats.

(b) HYPERSONIC AIRBREATHING WEAPON SYSTEM DEFINED.—In this section, the term ''hypersonic airbreathing weapon system'' means a missile or platform with military utility that operates at speeds near or beyond

approximately five times the speed of sound, and that is propelled through the atmosphere with an engine that burns fuel with oxygen from the atmosphere that is collected in an inlet.

SEC. 2___[Log 65538]. JOINT HYPERSONICS TRANSITION OFFICE.

(a) REDESIGNATION.—The joint technology office on hypersonics in the Office of the Secretary of Defense is redesignated as the ''Joint Hypersonics Transition Office''. Any reference in a law (other than this section), map, regulation, document, paper, or other record of the United States to the joint technology office on hypersonics shall be deemed to be a reference to the Joint Hypersonics Transition Office.

(b) HYPERSONICS DEVELOPMENT.—Section 218 of the John Warner National Defense Authorization Act for Fiscal Year 2007 (Public Law 109–364; 10 U.S.C. 2358 note), as amended by section 1079(f) of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–192; 129 Stat. 999), is amended—

(1) in the heading of subsection (a), by striking ''JOINT TECHNOLOGY OFFICE ON HYPERSONICS'' and inserting ''JOINT HYPERSONICS TRANSITION OFFICE'';

(2) in subsection (a)—

(A) in the first sentence, by striking ''joint technology office on hypersonics'' and inserting

''Joint Hypersonics Transition Office (in this section referred to as the 'Office')''; and

(B) in the second sentence, by striking ''office'' and inserting ''Office'';

(3) in subsection (b), by striking ''joint technology office established under subsection (a)'' and inserting ''Office''; and

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

''(c) RESPONSIBILITIES.—In carrying out the program required by subsection (b), the Office shall do the following:

''(1) Coordinate and integrate current and future research, development, test, and evaluation programs and system demonstration programs of the Department of Defense on hypersonics.

''(2) Undertake appropriate actions to ensure—

''(A) close and continuous integration of the programs on hypersonics of the military departments and the Defense Agencies with the programs on hypersonics across the Federal Government; and

''(B) that both foundational research and developmental testing resources are adequate and well funded, and that facilities are made

available in a timely manner to support hypersonics research, demonstration programs, and system development.

''(3) Approve demonstration programs on hypersonic systems to speed the maturation and deployment of the systems to the warfighter,.

''(4) Ensure that any demonstration program on hypersonic systems that is carried out in any year after its approval under paragraph (3) is carried out only if certified under subsection (e) as being consistent with the roadmap under subsection (d).

''(5) Develop a well-defined path for hypersonic technologies to transition to operational capabilities for the warfighter.'';

(5) in subsection (d)(1), by striking ''joint technology office established under subsection (a)'' and inserting ''Office''; and

(6) in subsection (e)—

(A) in paragraph (1), by striking ''joint technology office established under subsection (a)'' and inserting ''Office''; and

(B) in paragraph (2), by striking ''joint technology office'' and inserting ''Office''.

SEC. 5___ [Log 65359]. CODIFICATION OF AUTHORITY TO CONDUCT FAMILY SUPPORT PROGRAMS FOR IMMEDIATE FAMILY MEMBERS OF MEMBERS OF THE ARMED FORCES ASSIGNED TO SPECIAL OPERATIONS FORCES.

(a) CODIFICATION OF EXISTING AUTHORITY.—Chapter 88 of title 10, United States Code, is amended by inserting after section 1788 a new section 1788a consisting of—

(1) a heading as follows:

"§ 1788a. Family support programs: immediate family members of members of special operations forces"; and

(2) a text consisting of subsections (a), (b), (d), and (e) of section 554 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66; 10 U.S.C. 1788 note), redesignated as subsections (a), (b), (c), and (d), respectively.

(b) FUNDING.—Subsection (c) of section 1788a of title 10, United States Code, as added and redesignated by subsection (a) of this section, is amended by striking ''specified'' and all that follows through the end of the subsection and inserting '', from funds available for Major

Force Program 11, to carry out family support programs under this section.''.

(c) ELIMINATION OF PILOT PROGRAM REFERENCES AND OTHER CONFORMING AMENDMENTS.—Section 1788a of title 10, United States Code, as added by subsection (a) of this section, is further amended—

(1) by striking ''Armed Forces'' each place it appears and inserting ''armed forces'';

(2) by striking ''pilot'' each place it appears;

(3) in subsection (a)—

(A) in the subsection heading, by striking ''PILOT''; and

(B) by striking ''up to three'' and all that follows through ''providing'' and inserting ''programs to provide''; and

(4) in subsection (d), as redesignated by subsection (a) of this section—

(A) in paragraph (2). by striking ''title 10, United States Code'' and inserting ''this title''; and

(B) in paragraph (3), by striking ''such title'' and inserting ''this title''.

(d) CLERICAL AMENDMENT.—The table of sections at the beginning of subchapter I of chapter 88 of title 10,

United States Code, is amended by inserting after the item relating to section 1788 the following new item:

"1788a. Family support programs: immediate family members of members of special operations forces.".

(e) CONFORMING REPEAL.—Section 554 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66; 10 U.S.C. 1788 note) is repealed.

SEC. 8___ [Log 65066]. CLARIFICATION TO OTHER TRANSACTION AUTHORITY.

(a) CLARIFICATION TO REQUIREMENT FOR WRITTEN DETERMINATIONS FOR PROTOTYPE PROJECTS.—Section 2371b(a)(2) of title 10, United States Code, is amended by striking ''for a prototype project'' each place such term appears and inserting ''for a transaction (for a prototype project)''.

(b) CLARIFICATION OF INCLUSION OF SMALL BUSINESSES PARTICIPATING IN SBIR OR STTR.—Section 2371b(d)(1)(B) of title 10, United States Code, is amended by inserting ''(including small businesses participating in a program described under section 9 of the Small Business Act (15 U.S.C. 638))'' after ''small businesses''.

SEC. 9___ [Log 65423]. RESPONSIBILITY OF THE CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE FOR RISK MANAGEMENT ACTIVITIES REGARDING SUPPLY CHAIN FOR INFORMATION TECHNOLOGY SYSTEMS.

Section 142(b)(1) of title 10, United States Code, is amended—

(1) in subparagraph (H), by striking ''and'' at the end;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

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

''(J) has the responsibilities for policy, oversight, guidance, and coordination for risk management activities for the Department regarding the supply chain for information technology systems.''.

SEC. 10___[Log 65074]. TERMINATION OF REQUIREMENT TO SUBMIT ANNUAL BUDGET JUSTIFICATION DISPLAY FOR DEPARTMENT OF DEFENSE COMBATING TERRORISM PROGRAM.

Section 229 of title 10, United States Code, is amended by adding at the end the following new subsection:

''(e) TERMINATION.—The requirement to submit a budget justification display under this section shall terminate on December 31, 2020.''.

SEC. 10___[Log 64998]. LIMITATION ON EXPENDITURE OF FUNDS FOR EMERGENCY AND EXTRAORDINARY EXPENSES FOR INTELLIGENCE AND COUNTER-INTELLIGENCE ACTIVITIES AND REPRESENTATION ALLOWANCES.

(a) RECURRING EXPENSES.—The first sentence of subsection (a) of section 127 of title 10, United States Code, is amended by inserting before the period at the end the following: ", and is not a recurring expense".

(b) LIMITATION.—Subsection (c) of such section is amended by adding at the end the following new paragraph:

"(4) Funds may not be obligated or expended in an amount in excess of $25,000 under the authority of subsection (a) or (b) for intelligence or counter-intelligence activities or representation allowances until the Secretary of Defense has notified the congressional defense committees and the congressional intelligence committees of the intent to obligate or expend the funds, and—

"(A) in the case of an obligation or expenditure in excess of $100,000, 15 days have elapsed since the date of the notification; or

"(B) in the case of an obligation or expenditure in excess of $25,000, but not in excess of $100,000,

five days have elapsed since the date of the notification.''.

(c) ANNUAL REPORT.—Subsection (d) of such section is amended—

(1) by striking ''to the congressional defense committees'' and all that follows through the period at the end and inserting an em dash; and

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

''(1) to the congressional defense committees a report on all expenditures during the preceding fiscal year under subsections (a) and (b); and

''(2) to the congressional intelligence committees a report on expenditures relating to intelligence and counter-intelligence during the preceding fiscal year under subsections (a) and (b).''.

(d) DEFINITION.—Such section is further amended by adding at the end the following new subsection:

''(e) DEFINITION OF CONGRESSIONAL INTELLIGENCE COMMITTEES.—In this section, the term 'congressional intelligence committees' means the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.''.

SEC. 12___. [LOG 65075] NATO COOPERATIVE CYBER DEFENSE CENTER OF EXCELLENCE.

(a) AUTHORIZATION.—Of the amounts authorized to be appropriated by this Act for fiscal year 2018 for support of North Atlantic Treaty Organization (in this section referred to as ''NATO'') operations, as specified in the funding tables in division D, not more than $5,000,000 may be obligated or expended for the purposes described in subsection (b).

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

(1) enhance the capability, cooperation, and information sharing among NATO, NATO member nations, and partners, with respect to cyber defense and warfare; and

(2) facilitate education, research and development, lessons learned and consultation in cyber defense and warfare.

(c) CERTIFICATION.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall certify to the Committees on Armed Services of the House of Representatives and the Senate that the

Secretary has assigned executive agent responsibility for the Center to an appropriate organization within the Department of Defense, and detail the steps being undertaken to strengthen the role of the Center in fostering cyber defense and warfare capabilities within NATO.

(d) BRIEFING REQUIREMENT.—The Secretary of Defense shall periodically brief the Committees on Armed Services of the House of Representatives and the Senate on the efforts of the Department of Defense to strengthen the role of the Center in fostering cyber defense and warfare capabilities within NATO.

SEC. 12___. [LOG 65076] NATO STRATEGIC COMMUNICATIONS CENTER OF EXCELLENCE.

(a) AUTHORIZATION.—Of the amounts authorized to be appropriated by this Act for fiscal year 2018 for support of North Atlantic Treaty Organization (in this section referred to as ''NATO'') operations, as specified in the funding tables in division D, not more than $5,000,000 may be obligated or expended for the purposes described in subsection (b).

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

(1) enhance the capability, cooperation, and information sharing among NATO, NATO member nations, and partners, with respect to strategic communications and information operations; and

(2) facilitate education, research and development, lessons learned, and consultation in strategic communications and information operations.

(c) CERTIFICATION.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall certify to the Committees on Armed Services of the House of Representatives and the Senate that the

Secretary has assigned executive agent responsibility for the Center to an appropriate organization within the Department of Defense, and detail the steps being undertaken to strengthen the role of Center in fostering strategic communications and information operations within NATO.

(d) BRIEFING REQUIREMENT.—

(1) IN GENERAL.—The Secretary of Defense shall periodically brief the committees listed in paragraph (2) on the efforts of the Department of Defense to strengthen the role of the Center in fostering strategic communications and information operations within NATO.

(2) COMMITTEES.—The committees listed in this paragraph are the following:

(A) The Committee on Armed Services and the Committee on Foreign Affairs of the House of Representatives.

(B) The Committee on Armed Services and the Committee on Foreign Relations of the Senate.

SEC. 13___.[Log 65072] SPECIFICATION OF COOPERATIVE THREAT REDUCTION FUNDS.

(a) FISCAL YEAR 2018 COOPERATIVE THREAT REDUCTION FUNDS DEFINED.—In this title, the term ''fiscal year 2018 Cooperative Threat Reduction funds'' means the funds appropriated pursuant to the authorization of appropriations in section 301 and made available by the funding table in division D for the Department of Defense Cooperative Threat Reduction Program established under section 1321 of the Department of Defense Cooperative Threat Reduction Act (50 U.S.C. 3711).

(b) AVAILABILITY OF FUNDS.—Funds appropriated pursuant to the authorization of appropriations in section 301 and made available by the funding table in division D for the Department of Defense Cooperative Threat Reduction Program shall be available for obligation for fiscal years 2018, 2019, and 2020.

SEC. 1302. [Log 65071] FUNDING ALLOCATIONS.

(a) IN GENERAL.—Of the $324,600,000 authorized to be appropriated to the Department of Defense for fiscal year 2018 in section 301 and made available by the funding table in division D for the Department of Defense Cooperative Threat Reduction Program established under section 1321 of the Department of Defense Cooperative Threat Reduction Act (50 U.S.C. 3711), the following amounts may be obligated for the purposes specified:

(1) For strategic offensive arms elimination, $12,100,000.

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

(3) For global nuclear security, $17,900,000.

(4) For cooperative biological engagement, $172,800,000.

(5) For proliferation prevention, $89,800,000.

(6) For activities designated as Other Assessments/Administrative Costs, $27,000,000.

(b) MODIFICATION TO CERTAIN REQUIREMENTS.—The Department of Defense Cooperative Threat Reduction Act (50 U.S.C. 3701 et seq.) is amended as follows:

(1) Section 1321(g)(1) (50 U.S.C. 3711(g)(1)) is amended by striking ''45 days'' and inserting ''15 days''.

(2) Section 1324 (50 U.S.C. 3714) is amended—

(A) in subsection (a)(1)(C), by striking ''45 days'' and inserting ''15 days''; and

(B) in subsection (b)(3), by striking ''45 days'' and inserting ''15 days''.

(3) Section 1335(a) (50 U.S.C. 3735(a)) is amended by striking ''or expended''.

SEC. 15___[Log 65077]. JOINT IMPROVISED EXPLOSIVE DEVICE DEFEAT FUND.

(a) USE AND TRANSFER OF FUNDS.—Subsection 1532(a) of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1091) is amended by striking ''fiscal years 2016 and 2017'' and inserting ''fiscal years 2016, 2017, and 2018''.

(b) EXTENSION OF INTERDICTION OF IMPROVISED EXPLOSIVE DEVICE PRECURSOR CHEMICALS AUTHORITY.—Subsection (c) of section 1532 of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239; 126 Stat. 2057) is amended—

(1) in paragraph (1), by striking ''and 2017'' and inserting ''2017, and 2018''; and

(2) in paragraph (4), by striking ''December 31, 2017'' and inserting ''December 31, 2018''.

SEC. 16___.[Log 65092] EXTENSION OF AUTHORITY TO ENGAGE IN CERTAIN COMMERCIAL ACTIVITIES.

Section 431(a) of title 10, United States Code, is amended by striking ''December 31, 2017'' and inserting ''December 31, 2023''.

SEC. 16___.[Log 65500] SUBMISSION OF AUDITS OF COMMERCIAL ACTIVITY FUNDS.

Section 432(b)(2) of title 10, United States Code, is amended—

(1) by striking ''promptly''; and

(2) by inserting before the period at the end the following: ''by not later than December 31 of each year''.

SEC. 16___[Log 65078]. PLAN TO INCREASE CYBER AND INFORMATION OPERATIONS, DETERRENCE, AND DEFENSE.

(a) FINDINGS.—Congress finds following:

(1) Cyber threats originating from the Asia-Pacific region targeting the United States and the allies of the United States have grown through the use of cyber intrusions, exfiltration, and espionage by China and North Korea.

(2) In February 2016, Admiral Harry Harris Jr., Commander of the United States Pacific Command, in his testimony noted ''increased cyber capacity and nefarious activity, especially by China, North Korea, and Russia underscore the growing requirement to evolve command, control, and operational authorities''.

(3) Admiral Harris stated ''that in order to fully leverage the cyber domain, PACOM requires an enduring theater cyber capability able to provide cyber planning, integration, synchronization, and direction of cyber forces.''.

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

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

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

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

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

SEC. 16___[Log 65264]. MODIFICATION TO QUARTERLY CYBER OPERATIONS BRIEFINGS.

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

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

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

(2) by adding at the end the following:

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

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

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

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

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

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

SEC. 16___[Log 65550]. CYBER SCHOLARSHIP PROGRAM.

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

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

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

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

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

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

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

''§ 2200e. Definitions

''In this chapter:

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

''(A) Offensive cyber operations.

''(B) Defensive cyber operations.

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

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

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

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

(d) CONFORMING AMENDMENTS.—

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

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

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

(i) in subsection (a), by striking ''Department of Defense information assurance

requirements'' and inserting ''the cyber requirements of the Department of Defense''; and

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

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

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

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

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

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

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

(2) The table of sections at the beginning of chapter 112 of title 10, Unites States Code, is

amended by striking the item relating to section 2200c and inserting the following:

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

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

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

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

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

(e) REDESIGNATIONS.—

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

(2) CENTERS OF ACADEMIC EXCELLENCE.—Any institution of higher education designated by

the Director of the National Security Agency as a Center of Academic Excellence in Information Assurance Education is redesignated as a Center of Academic Excellence in Cyber Education. Any reference in a law (other than this section), map, regulation, document, paper, or other record of the United States to a Center of Academic Excellence in Information Assurance Education shall be deemed to be a reference to a Center of Academic Excellence in Cyber Education.

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

SEC. 16___[Log 65657]. NOTIFICATION REQUIREMENTS FOR SENSITIVE MILITARY CYBER OPERATIONS AND CYBER WEAPONS.

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

"§ 130j. Notification requirements for sensitive military cyber operations

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

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

"(2) The congressional defense committees shall ensure that committee procedures designed to protect from

unauthorized disclosure classified information relating to national security of the United States are sufficient to protect the information that is submitted to the committees pursuant to this section.

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

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

''(A) is carried out by the armed forces or by a foreign partner in coordination with the armed forces; and

''(B) is intended to cause effects outside a geographic location where United States armed forces are involved in hostilities (as that term is used in section 1543 of title 50, United States Code).

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

''(A) An offensive cyber operation.

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

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

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

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

''(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide any new authority or to alter or otherwise affect the War Powers Resolution (50 U.S.C. 1541 et seq.), the Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note), or any requirement under the National Security Act of 1947 (50 U.S.C. 3001 et seq.).

''§ 130k. Notification requirements for cyber weapons

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

''(1) With respect to a cyber capability that is intended for use as a weapon, the results of any review of the capability for legality under international law pursuant to Department of Defense Directive 5000.01 no later than 48 hours after any military department concerned has completed such review.

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

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

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

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

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

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

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

''(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide any new authority or to alter or otherwise affect the War Powers Resolution (50 U.S.C. 1541 et seq.), the Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note), or any requirement under the National Security Act of 1947 (50 U.S.C. 3001 et seq.).''.

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

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

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

Rapid integration for emerging threats against missile system networks

The committee is aware that there are a number of rapidly emerging threats to the integrity and security of space and missile systems and their associated networks. The committee recognizes that the Program Executive Office for the Army Missile and Space Command is developing a capability to provide cyber-robust networked weapon systems the ability to assess and integrate rapid countermeasures to such threats. The committee understands this capability is accomplished through a unique approach to adapt to real-time threats, dramatically accelerating the timeline to employ resilience in networked weapon systems. Therefore, the committee directs the Secretary of the Army to provide a briefing to the Committee on Armed Services of the House of Representatives by March 1, 2018, on the status of progress being made through this accelerated program.

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, NAVY

Items of Special Interest

Naval energetic materials roadmap

The committee is aware that energetic materials, including both explosives and propellants, are critical components to Navy weapon systems and munitions. While the committee is aware that Navy laboratories and engineering centers have been involved in some research into energetic materials, the committee is concerned that these investments have not been strategic in scope or direction. Much of the ongoing work is devoted to sustaining legacy formulations for energetic materials, not investing in new or revolutionary propellants or explosives.

Therefore, the committee believes that the Navy should pursue a renaissance of its energetic materials enterprise and directs the Secretary of the Navy to develop a long-term science and technology roadmap for the development of energetic materials, both explosives and propellants. In developing this roadmap, the committee believes that Navy should consider the identification of the long-term research opportunities for the Navy for energetic materials; an assessment of the current laboratory and engineering infrastructure to meet the needs of this roadmap; and a resourcing strategy. The committee further directs the Secretary of

the Navy to provide a briefing to the House Committee on Armed Services by March 2, 2018, on the plan.

Workforce management at Navy test ranges

The committee notes that Navy elements of the Major Range and Test Facility Base (MRTFB) operate under the Navy Working Capital Fund (WCF). As such, their workforce management should be dictated by section 2208 of title 10, United States Code, which allows for flexibility in decisions to expand the workforce driven by the funded work coming in from other Navy or government customers. However, other parts of the MRTFB, which in the other military services do not operate in a WCF, use a billeting system to manage the workforce. The committee notes that such conflicting workforce management methods can prove to be problematic when funding work across the MRTFB enterprise. The committee is concerned that this uncertainty may be posing challenges for planning at these Navy test ranges.

Therefore, the committee directs the Secretary of the Navy to provide a briefing to the House Committee on Armed Services by October 2, 2017, on the workforce management policies at Navy MRTFBs, including any shortfalls in staffing, conflicts in guidance between WCF organizations and MRTFB organizations, and recommendations for improving hiring and talent management at these facilities.

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

Items of Special Interest

Accumulation of section 219 funds

The committee is aware that section 219 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110-417) provided new authorities to allow the Department of Defense laboratories to set aside funds for activities to improve the labs' ability to conduct defense missions. That authority included the use of these funds for some minor military construction projects that would help alleviate the backlog in modernization needed to keep the labs at the cutting edge of research. The provision was further modified by section 262 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113-66) to allow these funds to be accumulated for up to 5 years.

However, the committee is aware that to date, no actions have been taken to implement the new authority allowing the accumulation of funds among any of the military services. While there has been some discussion about difficulty in establishing the accounting procedures to account for these funds, the committee is not aware of any formal determination or explanation of the reasons for not implementing this authority. The committee is concerned that the Department, despite the widespread support for these authorities among the Department of

Defense laboratories, has not provided sufficient attention to this issue to work through any difficulties. Therefore, the committee directs the Secretary of Defense, in coordination with the Secretaries of the military departments, to provide a briefing to the House Committee on Armed Services by January 15, 2018, on the status and challenges of implementing subsection (b)(3) of section 219 of Public Law 110-417, including recommendations for actions that might support implementation.

Additive manufactured parts

The committee is aware of the significant possibilities that additive manufacturing, or 3-D printing, will provide to the Department of Defense, both in revolutionizing the industrial supply chain, as well as in providing radically new technological capabilities. The ability to utilize new materials in new ways, such as titanium or explosives, or to develop new manufacturing processes, has the potential to transform how the Department does business. The establishment of new Defense Manufacturing Innovation Institutes, as well as the growing prevalence of 3-D printers at tactical levels, indicates the Department sees that potential as well. Additive manufacturing could also greatly improve the organic industrial base's ability to respond to demands that original equipment manufacturers are unable to meet or to fabricate obsolete parts that are no-longer manufactured.

The committee understands that an inhibitor to seeing the full potential of this technology will be the need to do quality assurance and validation of additive manufactured parts, especially for those in flight or safety-critical systems. Until the Department can develop the standards and processes for assuring quality, 3-D printing will be limited in its application. Also, substantial room remains across the force to add more capacity for this capability, both to repair out-of-date equipment and to speed repair in order to meet urgent operational requirements.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than December 1, 2017, on the Department's plans to develop and improve additive manufacturing. The briefing shall include the Department's plans to: develop military and quality assurance standards as quickly as possible; leverage current manufacturing institutes to conduct research in the validation of quality standards for additive manufactured parts; and further integrate additive manufacturing capabilities and capacity into the Department's organic depots, arsenals, and shipyards.

Medical simulation research

The committee is aware that medical simulation systems can improve education, training, and skills development. While many of the current simulator manikins used for practical, hands-on training lack the tactile fidelity and accurate portrayal of multiple biological and organ systems, these systems hold greater promise in the future after further development and validation. However, recent

advances in computational power, big data analytics, machine learning, and medical informatics also indicate promise for new forms of medical simulation that might be applied to other areas of clinical outcomes, including clinical decision support.

The committee is encouraged by advances in both areas, and believes the Department of Defense could do more to leverage these technological advances to support medical training. Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by January 19, 2018, on current investments in medical simulation technology and research and Department-wide efforts to incorporate simulated learning techniques in defense medical training.

TITLE X—GENERAL PROVISIONS

ITEMS OF SPECIAL INTEREST

OTHER MATTERS

Comptroller General Assessment of Emerging Threats of High National Security Consequence

Within the next ten years, the committee believes that several challenges could present emerging threats of high national security consequence, such as: the proliferation of disruptive and exponentially deployed technologies; the introduction of novel asymmetric weapons; second and third-order effects of environmental and climate-related issues; global pandemic and public health issues; shifting demographics and urbanization effects; and unanticipated state and non-state acts of aggression.

Since the committee believes the Department of Defense must be prepared to counter these threats, the committee directs the Comptroller General of the United States to identify and assess these and other emerging threats that could affect the national security of the United States. Such an assessment should provide a snapshot of critical emerging threats based on the views of the intelligence community, combatant commands, and other Department of Defense organizations, such as the Defense Advanced Research Projects Agency and the Defense Threat Reduction Agency. The assessment should identify:

(1) the emerging threats within each geographic combatant commander's area of responsibility;

(2) the extent to which the threats are highlighted in current national security defense strategies; and

(3) the Department's component(s), if any, tasked to monitor and mitigate these threats.

The committee directs the Comptroller General to provide a briefing to the congressional defense committees by February 1, 2018, on preliminary findings, with a report to follow.

Requirement for Notification of Modifications Made to Presidential Policy Guidance for Direct Action Against Terrorist Targets

When necessary, U.S. Armed Forces use lethal force abroad to protect the American people, consistent with American values and all applicable law, including the international laws of armed conflict. In 2013, the Administration issued Presidential Policy Guidance (PPG) establishing standard operating procedures for direct action, which refers to lethal and non-lethal uses of force, including capture operations against terrorist targets in areas of active hostilities outside of the United States. The committee is aware that the current Administration has directed the Department of Defense and the interagency to review the procedures for direct action against terrorist targets established by the 2013 PPG, and that the results of this review are forthcoming.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services within 30 days of any change made to procedures for direct action against terrorist targets conducted under title 10, United States Code, authorities, including any deviation, variation, change, or termination of procedure outlined within the 2013 PPG. Additionally, the committee expects the Secretary of Defense to continue to comply with standing requirements to notify the congressional defense committees of non-combatant causalities associated with direct action activities conducted under the auspices of the PPG, and all other title 10 operations, to include a year-end compilation by country.

U.S. Efforts to Train, Advise, Assist, and Equip the Iraqi Counterterrorism Service and the Iraqi Special Operations Forces

The committee has received from the Inspector General of the Department of Defense the report entitled, "An Assessment of U.S. and Coalition Plans and Efforts to Train, Advise, Assist, and Equip the Iraqi Counterterrorism Service and the Iraqi Special Operations Forces" (DODIG-2017-074). Although the report found no statutory anomalies with the implementation of Iraqi train and equip efforts, the committee is concerned that several findings indicated a lack of accountability with materiel and equipment, training standards, and training metrics specifically for the Iraqi Counterterrorism Service and the Iraqi Special Operations Forces. Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by September 1, 2017, on his plan to implement the recommendations made in DODIG-2017-074 concerning efforts to train, advise, assist, and equip the Iraqi Counterterrorism Service and the Iraqi Special Operations Forces.

TITLE XIV—OTHER AUTHORIZATIONS

ITEMS OF SPECIAL INTEREST

Assessment of the Realignment of the Joint Improvised-Threat Defeat Organization under the Defense Threat Reduction Agency

The committee supports the transition of the Joint Improvised-Threat Defeat Agency (JIDA) to the Defense Threat Reduction Agency (DTRA) as the Joint Improvised-Threat Defeat Organization (JIDO) under DTRA. The committee also appreciates actions taken to achieve efficiencies and synergies while not compromising the mission of either JIDO or DTRA and without interruption of support to the warfighter. However, the committee believes there may be opportunities for additional efficiencies and collaboration that can be achieved as a result of this transition.

For example, the committee is aware JIDO has taken on a greater role in countering unmanned aerial systems (UAS). The committee recognizes the nexus between UAS and improvised explosive devices (IEDs). However, the committee is concerned about mission creep to countering weapon systems and platforms that may diminish focus on the mission of countering IEDs employed in all forms. Additionally, the JIDO director remains a two-star billet sourced by the Army. The committee is concerned about whether this level of seniority for JIDO is necessary given the leadership and oversight structures in place at DTRA.

Therefore, the committee directs the Comptroller General of the United States to assess the transition of JIDA as JIDO to DTRA, to include an assessment of additional efficiencies that may be achieved and recommendations for progress to that end in the near-term, as well as an assessment of JIDA's primary mission of countering current and future IED threats. The Comptroller General shall provide a briefing to the congressional defense committees, not later than March 1, 2018, on the results of the assessment with a report to follow on a date agreed to at the time of the briefing.

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

ITEMS OF SPECIAL INTEREST

CYBER-RELATED MATTERS

Assessment of Effectiveness of Cyber Reporting

The committee is aware that the Department of Defense has been working for several years to develop a new cyber security and incident reporting scheme for defense contractors with access to controlled, unclassified information stored on, or

processed by, their own information networks. While this requirement is called for by section 941 of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112-239), the Department has drafted and promulgated a new contract clause in the Defense Federal Acquisition Regulation Supplement (DFARS) as a means to implement the requirements of this reporting.

The committee is aware that this new language, DFARS 252.204-7012 on Cyber Security and Incident Reporting, has been the cause of concern and misunderstanding from many in industry, particularly among small businesses, and those businesses where defense revenue is a very small percentage of their overall revenue. The committee acknowledges that the Department has made efforts to make this new guidance as easy to implement and track as possible, and understands that the new process provides wide latitude and flexibility for businesses to craft strategies for compliance. For example, the Department has made available a number of tools to help small businesses with implementation, and worked extensively with Procurement Technical Assistance Centers so they can understand the requirements and assist small businesses directly in the course of their normal support. Additionally, the Department of Homeland Security has updated and modified their Cyber Security Evaluation Tool to provide a means for businesses to self-evaluate their compliance with the new rules.

To ensure that these tools are effective at helping small businesses and other non-traditional defense contractors meet this requirement, the committee directs the Secretary of Defense to conduct an assessment of the DFARS clause. The Secretary should assess the compliance of industry, including the extent to which these support tools have been effective. This assessment should also identify any issues and concerns with the quality of System Security Plans from the contractors, and to the extent practicable, should include input from affected contractors. The committee further directs the Secretary to provide a briefing to the House Committee on Armed Services by December 7, 2018, on the results of this assessment.

Cloud Computing

The committee believes the widespread adoption by the Department of Defense of cloud computing technology would be beneficial to both the management functions and operational functions of the Department of Defense, resulting in cost savings, increased flexibility and scalability, mobility, and improved security. For example, cloud computing provides enhanced data analytics capabilities, reduces the need for physical data storage centers, and increases situational awareness on the battlefield. The committee is pleased that the military departments, particularly the Department of the Navy and Department of the Army, have recognized cloud computing is not only beneficial to the enterprise, but can also provide increased warfighting capabilities for tactical and operational advantages.

The committee encourages the continued use of cloud computing to achieve battlefield advantages, and encourages the Department of Defense to use cloud

computing in military exercises and wargaming. For example, the Department of Defense could examine the use of cloud computing to support continuity of operations planning or to support resilient operations in the face of a degraded cyber environment. The committee also encourages greater synergy and collaboration between the acquisition community and information technology community, so that future weapon systems and platforms take full advantage of cloud computing benefits.

Additionally, the committee supports the less risk-averse approach by the military services, than is traditionally prevalent throughout the Department of Defense, to incorporate cloud computing at the tactical, operational, strategic, and enterprise-wide levels. The committee believes the Department of Defense Chief Information Office should leverage lessons learned by the military services on cloud computing, to include security, capabilities, and criteria to appropriately determine if commercial, government, or hybrid clouds are required to update the Department's cloud strategy and assess current Department of Defense cloud security requirements; specifically, on-premise and off-premise requirements.

Finally, the committee directs the Department of Defense's Chief Information Officer to provide a briefing to the House Committee on Armed Services by March 5, 2018, on cloud computing. The briefing should include efforts to coordinate with the acquisition community, encourage the use of cloud computing in wargaming and military exercises, and an assessment of the Department of Defense's current cloud strategy and security requirements.

Comptroller General Assessment of Cyber Training

The committee is aware that the military services have been developing cyber training standards and establishing cyber schools or centers of excellence to prepare their personnel for operations in cyberspace. While the services have responsibility to train their forces, these forces must be trained to consistent and joint standards. The committee believes that the military services should leverage each other's training capabilities to the extent possible.

Therefore, the committee directs the Comptroller General of the United States to assess the Department of Defense's current and planned state of cyber training. The assessment should identify the extent to which the military services:

(1) have established consistent cyber training standards for Active and Reserve Component forces;

(2) have leveraged each other's cyber training capabilities, to include training schools and ranges;

(3) are achieving training capability and capacity goals; and

(4) are leveraging other cyber experience to meet training requirements.

The committee directs the Comptroller General to provide a briefing to the House Committee on Armed Services by March 15, 2018, on preliminary findings, with a report to follow on a date agreed to at the time of the briefing.

Data Protection

The committee remains concerned about continuing reports of unauthorized disclosures of critical program and other classified information, whether from insiders or from external network intrusions. While the Department of Defense has made significant investments to improve its cyber security posture, the committee also remains concerned by the rate of progress the Department is making in preventing unauthorized review, redistribution, and modification of sensitive government information. The committee recognizes that there are a number of technologies, such as digital rights management (DRM) and attribute-based access control (ABAC), that could provide useful, needed capabilities in the Joint Information Environment, and are specifically cited as new information security policy requirements to help intelligence and civilian agencies persistently protect their sensitive information and high-value asset data both inside and outside of agency networks.

Therefore, the committee directs the Department of Defense Chief Information Officer, in coordination with the Director of the Defense Information Systems Agency, to provide a briefing to the House Committee on Armed Services by November 1, 2017, on any current plans to demonstrate or incorporate Department-wide DRM and ABAC capabilities into upgrades to key enabling cyber capabilities inside the Joint Regional Security Stacks initiative.

Implementation of Recommendations by Defense Science Board Task Force on Cyber Deterrence and Cyber Supply Chain

The committee has reviewed the findings and recommendations contained in the Defense Science Board Task Force on Cyber Deterrence report and the Defense Science Board Task Force on Cyber Supply Chain report. The committee appreciates these comprehensive and substantive reviews that contain tangible recommendations for the Department of Defense in the areas of cybersecurity, deterrence, supply chain vulnerabilities, and other related issues. Over the previous several years, the committee has provided the Department with multiple new or revised authorities, as well as significant funding, to address many of the challenges identified in these two reports. The committee is concerned, however, that the Department nonetheless lacks a comprehensive strategy to implement many of the important recommendations contained in these two Defense Science Board reports on cyber.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by September 1, 2017, on efforts to implement the recommendations contained in the Defense Science Board Task Force on Cyber Deterrence and the Defense Science Board Task Force on Cyber Supply Chain reports.

Persistent Training Environment

The committee is aware that the development of a Persistent Training Environment (PTE) for cyber is a significant priority for U.S. Cyber Command. The committee recognizes that the Department of Defense is currently struggling to train, certify, and deploy sufficient personnel to man to the levels called for by the Cyber Mission Force (CMF) construct.

Further, the committee recognizes the need for periodic recertification for both individuals and teams to keep skills sharp. In order to meet this demand, the committee believes it will be critical to develop the PTE to provide the means to enable thousands of military and civilian personnel to maintain their skills and certification required to continue to work on missions.

Therefore, the committee directs the Commander of U.S. Cyber Command, in coordination with the Secretary of the Army, to provide a briefing to the House Committee on Armed Services by December 8, 2017, on the progress in developing the PTE. This briefing should address the capability goals for the program, funding profile, major projected milestones (including any exercises PTE is expected to be used in conjunction with), performers, and any significant risks to the program.

INTELLIGENCE MATTERS

Distributed Common Ground System Special Operations Forces

The committee is aware that U.S. Special Operations Command is pursuing an effort under the Distributed Common Ground System-Special Operations Forces (DCGS-SOF) program to unify SOF intelligence community capabilities under a common, commercially available backbone solution and integrate SOF-unique capabilities. The committee notes that in previous oversight on this program, the Department of Defense described an acquisition approach that "leverages SOF programs, DOD partners, and other government agencies to integrate COTS [commercial-off-the-shelf], GOTS [government-off-the-shelf], and other mature technologies" using a best of breed methodology for seamless integration and federation, as well as an "agile development process with capability insertions into the development baseline for assessment and future deployment into the operational baseline."

Further, the committee understands that this program has leveraged a common commercial practice by structuring the request for proposals to provide usable software for evaluation, vice a written response describing capabilities. The award was based on comparison of software provided to the listed requirements, and thus the award was primarily for the deployment of the solution, with development limited to integration. The committee believes this approach is a good model for the Department as it relates to software intensive systems, especially the approach to obtaining systems that allow the lead integrator to have access to proprietary information and data in order to avoid unnecessary costs and allow for continued open competition.

The committee directs the Commander, U.S. Special Operations Command to provide a briefing to the House Committee on Armed Services and the House Permanent Select Committee on Intelligence by October 31, 2017, updating progress in deployment of this capability, as well as how lessons learned from the program are being shared more broadly within the information technology acquisition community.