

H.R. 4909—FY17 NATIONAL DEFENSE AUTHORIZATION BILL

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

SUMMARY OF BILL LANGUAGE.....	1
BILL LANGUAGE.....	13
DIRECTIVE REPORT LANGUAGE	71

SUMMARY OF BILL LANGUAGE

Table Of Contents

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE I—PROCUREMENT

LEGISLATIVE PROVISIONS

SUBTITLE E—DEFENSE-WIDE, JOINT, AND MULTISERVICE MATTERS

Section 1xx—Termination of Quarterly Reporting on Use of Combat Mission Requirements Funds

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

LEGISLATIVE PROVISIONS

SUBTITLE B—PROGRAM REQUIREMENTS, RESTRICTIONS, AND LIMITATIONS

Section 2xx—Limitation on Availability of Funds for Defense Innovation Unit Experimental

Section 2xx—Prohibition on Availability of Funds for Countering Weapons of Mass Destruction System Constellation

Section 2xx—Improved Biosafety for Handling of Select Agents and Toxins

Section 2xx—Modernization of Security Clearance Information Technology Architecture

SUBTITLE C—OTHER MATTERS

Section 2xx—Strategy for Assured Access to Trusted Microelectronics

Section 2xx—Laboratory Quality Enhancement Program

Section 2xx—Pilot Program on Evaluation of Commercial Information Technology

Technology

Section 2xx—Report on Electronic Warfare Capabilities

TITLE VIII—ACQUISITION POLICY, ACQUISITION

MANAGEMENT, AND RELATED MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE B—INDUSTRIAL BASE MATTERS

Section 8xx—Amendments Related to Detection and Avoidance of Counterfeit Electronic Parts

SUBTITLE C—OTHER MATTERS

Section 8xx—Review of Anti-Competitive Specifications in Information Technology Acquisitions

TITLE X—GENERAL PROVISIONS

LEGISLATIVE PROVISIONS

SUBTITLE D—COUNTERTERRORISM

Section 10xx—Matters for Inclusion in Report on Designation of Countries for which Rewards May Be Paid under Department of Defense Rewards Program

Section 10xx—Frequency of Counterterrorism Operations Briefings

SUBTITLE H—OTHER MATTERS

Section 10xx—Congressional Notification of Biological Select Agent and Toxin Theft, Loss, or Release Involving the Department of Defense

Section 10xx—Report on Service-Provided Support to United States Special Operations Forces
Section 10xx—National Biodefense Strategy
Section 10xx—Report on Counterproliferation Activities and Programs
Section 10xx—Two-Year Extension and Modification of Authorization of Non-Conventional Assisted Recovery Capabilities

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

LEGISLATIVE PROVISIONS

SUBTITLE G—OTHER MATTERS

Section 12xx—Extension of Authority for Support of Special Operations to Combat Terrorism
Section 12xx—Authority to Destroy Certain Specified World War II-Era United States-Origin Chemical Munitions Located on San Jose Island, Republic of Panama
Section 12xx—Modification and Extension of Authority to Conduct Activities to Enhance the Capability of Foreign Countries to Respond to Incidents Involving Weapons of Mass Destruction

TITLE XV—AUTHORIZATION OF ADDITIONAL APPROPRIATIONS FOR OVERSEAS CONTINGENCY OPERATIONS

LEGISLATIVE PROVISIONS

SUBTITLE D—LIMITATIONS, REPORTS, AND OTHER MATTERS

Section 15xx—Joint Improvised Explosive Device Defeat Fund
Section 15xx—Extension of Authority to Use Joint Improvised Explosive Device Defeat Fund for Training of Foreign Security Forces to Defeat Improvised Explosive Devices

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE C—CYBERSPACE-RELATED MATTERS

Section 16xx—Special Emergency Procurement Authority to Facilitate the Defense Against or Recovery from a Cyber Attack
Section 16xx—Change in Name of National Defense University's Information Resources Management College to College of Information and Cyberspace
Section 16xx—Requirement to Enter into Agreements Relating to Use of Cyber Opposition Forces
Section 16xx—Limitation on Availability of Funds for Cryptographic Systems and Key Management Infrastructure

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE I—PROCUREMENT

LEGISLATIVE PROVISIONS

SUBTITLE E—DEFENSE-WIDE, JOINT, AND MULTISERVICE MATTERS

Section 1xx—Termination of Quarterly Reporting on Use of Combat Mission Requirements Funds

This section would amend the quarterly report requirement in section 123 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111-383), to sunset the requirement for such reports on September 30, 2018.

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

LEGISLATIVE PROVISIONS

SUBTITLE B—PROGRAM REQUIREMENTS, RESTRICTIONS, AND LIMITATIONS

Section 2xx—Limitation on Availability of Funds for Defense Innovation Unit Experimental

This section would limit the amount of authorized funds available to be obligated or expended for the Defense Innovation Unit Experimental (DIUx) until the Secretary of Defense provides a report to the congressional defense committees on the charter for and the use of funds to establish and expand DIUx.

The committee is aware of the Department of Defense's efforts to increase outreach to and collaboration with sources of commercial innovation throughout the United States. The committee recognizes that commercial innovation is not only a significant driver for the economy, but also provides significant contributions to national security. The committee has been supportive of mechanisms for tapping into the nontraditional defense contractor community, which includes commercial start-ups and other companies that have not typically focused on the defense market. The committee notes that the administrative and regulatory barriers that are in place within the acquisition system often act as moats to keep these innovation players out, rather than a bridge into the national security sector.

The committee believes DIUx to be a helpful step in bridging those communities, but is concerned by the pinpoint focus on one geographic region, as well as the dedication of significant funding at such a nascent period in the

development of this organization and the concept on which it was founded. The committee is concerned that outreach is proceeding without sufficient attention being paid to breaking down the barriers that have traditionally prevented nontraditional contractors from supporting defense needs, like lengthy contracting processes and the inability to transition technologies. Furthermore, the committee is concerned that the focus on this initiative is occurring without sufficient guidance, oversight, and coordination with and into the various laboratories, engineering centers, and existing state and local innovation centers that by necessity must also bridge into this community. The committee believes that focusing on laying a solid foundation for DIUX and its interaction with communities and the Department of Defense enterprise is critical to ensuring effectiveness, especially if such initiatives will be expanded to include other locations.

Section 2xx—Prohibition on Availability of Funds for Countering Weapons of Mass Destruction System Constellation

This section would prohibit the Department of Defense from obligating or expending any funds in fiscal year 2017 for research, development, and prototyping of the countering weapons of mass destruction situational awareness information system, known as "Constellation." This section would also require the Chief Information Officer of the Department of Defense, in consultation with the Director of the Defense Information Systems Agency, to submit a report to the congressional defense committees by February 1, 2017, on the requirements and program plan for the Constellation system.

Section 2xx—Improved Biosafety for Handling of Select Agents and Toxins

This section would direct the Department of Defense to implement several improvements for handling of select agents and toxins, as recommended from an Army 15-6 investigative report on the individual and institutional accountability for the shipment of viable Bacillus Anthracis from Dugway Proving Ground. This section would require the Department to implement a quality assurance and quality control program for any facility producing biological select agents and toxins, and for the Secretary of Defense to submit a report to the congressional defense committees by February 1, 2017, on the potential consolidation of facilities that work with biological select agents and toxins. This section would also require the Comptroller General of the United States to submit a report to the congressional defense committees by September 1, 2017, on the effectiveness and completeness of the Department of Defense's actions taken to address the findings and recommendations of the Army 15-6 investigation.

Section 2xx—Modernization of Security Clearance Information Technology Architecture

This section would require the Secretary of Defense to develop and sustain a new security clearance information technology architecture to replace the legacy system of the Office of Personnel Management. Further, this section would require the Secretary of Defense, Director of National Intelligence, and Director of the Office of Personnel Management to issue a governance charter to delineate responsibilities between organizations, as well as to review and revise as necessary the executive orders, statutes, and other authorities related to personnel security. This section would also require quarterly notifications to designated congressional committees until September 30, 2019.

SUBTITLE C—OTHER MATTERS

Section 2xx—Strategy for Assured Access to Trusted Microelectronics

This section would require the Secretary of Defense to develop and implement a strategy for developing and acquiring trusted microelectronics from various sources by 2020. This section would further require the Secretary to submit such a strategy to the congressional defense committees not later than 1 year after the date of the enactment of this Act. The Secretary of Defense would also be required to certify by September 30, 2020, that the Department has implemented the recommendations of the strategy, and has created an assured means of accessing sufficient supply of trusted microelectronics.

Section 2xx—Laboratory Quality Enhancement Program

This section would require the establishment of a Laboratory Quality Enhancement Program (LQEP) to support the analysis and implementation of current policies, as well as make recommendations for new initiatives to support the improvement and enhancement of the Department of Defense's Science and Technology Reinvention Laboratories. This section would also place responsibility for LQEP under the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)), and would modify section 1114(a)(2)(C) in the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Public Law 106-398) to align management of the laboratory demonstration program with the ASD(R&E).

Section 2xx—Pilot Program on Evaluation of Commercial Information Technology

This section would require the Defense Information Systems Agency to establish a pilot program to evaluate commercially available information technology tools to better understand and characterize their potential impact on Department of Defense networks and computing environments through prototyping,

experimentation, operational demonstration, military user assessment, or other means to get quantitative and qualitative feedback on the commercial item.

Section 2xx—Report on Electronic Warfare Capabilities

This section would require the Under Secretary of Defense for Acquisition, Technology, and Logistics, acting through the Electronic Warfare Executive Committee, to submit to the congressional defense committees a report by April 1, 2017, on future electronic warfare concepts and technologies. The report shall include a strategy for developing and implementing new operational concepts, synchronization and oversight of current and future programs, training and operational support requirements, and methods for securing technological advances.

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

LEGISLATIVE PROVISIONS

SUBTITLE B—INDUSTRIAL BASE MATTERS

Section 8xx—Amendments Related to Detection and Avoidance of Counterfeit Electronic Parts

This section would modify section 818 of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112-81) by replacing the term "trusted suppliers" with the term "suppliers that meet anticounterfeiting requirements", as well as related conforming amendments.

The committee is aware that the term "trusted" in this context has created some confusion, since "trusted suppliers" refers to a specific category of microelectronics suppliers that have been accredited by the Defense Microelectronics Activity. Counterfeit parts refer to a much broader set of circumstances and require a broader definition of the supplier base needed to address counterfeiting concerns.

SUBTITLE C—OTHER MATTERS

Section 8xx—Review of Anti-Competitive Specifications in Information Technology Acquisitions

This section would require the Under Secretary of Defense for Acquisition, Technology, and Logistics to review the policy, guidance, regulations, and training related to specifications included in information technology (IT) acquisitions within 180 days after the date of the enactment of this Act. The purpose of this review would be to ensure that current policies eliminate the use of potentially anti-

competitive specifications, such as the use of brand name procurements, or references to proprietary specification or standards in IT acquisitions. This section would also require the Under Secretary to provide a briefing to the Senate Committee on Armed Services and the House Committee on Armed Services on the review. Lastly, this section would require the Under Secretary to revise current policies, guidance, and training to incorporate any recommended changes from this review, should changes be warranted.

TITLE X—GENERAL PROVISIONS

LEGISLATIVE PROVISIONS

SUBTITLE D—COUNTERTERRORISM

Section 10xx—Matters for Inclusion in Report on Designation of Countries for which Rewards May Be Paid under Department of Defense Rewards Program

This section would modify the reporting requirements in section 127b(h) of title 10, United States Code, for the Department of Defense Rewards Program to clarify the requirement to report on the designation of countries for which rewards or payment-in-kind may be paid.

Section 10xx—Frequency of Counterterrorism Operations Briefings

This section would amend section 485 of title 10, United States Code, to require the Secretary of Defense to provide monthly counterterrorism operations briefings to the congressional defense committees.

SUBTITLE H—OTHER MATTERS

Section 10xx—Congressional Notification of Biological Select Agent and Toxin Theft, Loss, or Release Involving the Department of Defense

This section would direct the Secretary of Defense to provide notification to the congressional defense committees within 15 days of notifying the Centers for Disease Control and Prevention and/or the Animal and Plant Health Inspection Service of any theft, loss, or release of biological select agents or toxins.

Section 10xx—Report on Service-Provided Support to United States Special Operations Forces

This section would require the Secretary of Defense to submit a report to the congressional defense committee within 180 days after the date of the enactment of this Act on support contributed from each of the military services towards special operations forces for each of the fiscal years 2018-20.

Section 10xx—National Biodefense Strategy

This section would require the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Homeland Security, and the Secretary of Agriculture to jointly develop and submit to the appropriate congressional committees, within 275 days of the date of the enactment of this Act, a national biodefense strategy and implementation plan. This section would also require the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Homeland Security, and the Secretary of Agriculture to provide a joint briefing to the appropriate congressional committees annually, starting March 1, 2017, and ending March 1, 2019, on the strategy and status of its implementation. This section would also require the Comptroller General of the United States to submit a report to the appropriate congressional committees, within 180 days of submission of the national biodefense strategy, on a gap analysis of the national biodefense strategy and its implementation plan.

Section 10xx—Report on Counterproliferation Activities and Programs

This section would require the Secretary of Defense to provide the congressional defense committees with a biennial report, with a sunset date of January 31, 2021, on the Department of Defense's counterproliferation activities and programs. This report would be a simplified replacement for the Counterproliferation Program Review Committee report from section 1603 of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103-160) that has recently expired. The content of this report is aimed to reduce the reporting burden on the Department, while still providing the congressional defense committees with program analysis critical for robust program oversight.

Section 10xx—Two-Year Extension and Modification of Authorization of Non-Conventional Assisted Recovery Capabilities

This section would modify section 943 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110-417), as most recently amended by section 1271 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92), to permit the recovery of individuals identified by the Secretary of Defense when a non-conventional assisted recovery capability is already in place. This section would also extend the authority through 2020.

The committee reminds the Department that this authority constitutes a traditional military activity for personnel recovery and should not be interpreted as an intelligence activity. The committee notes that failure to use and report this authority accordingly will jeopardize future re-authorizations.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

LEGISLATIVE PROVISIONS

SUBTITLE G—OTHER MATTERS

Section 12xx—Extension of Authority for Support of Special Operations to Combat Terrorism

This section would modify and extend section 1208(h) of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Public Law 108-375), as most recently amended by section 1208(b) of the Carl Levin and Howard P. “Buck” McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113-291), for 3 years, through fiscal year 2020.

Section 12xx—Authority to Destroy Certain Specified World War II-Era United States-Origin Chemical Munitions Located on San Jose Island, Republic of Panama

This section would authorize the Secretary of Defense to destroy the eight U.S.-origin chemical munitions on San Jose Island, Republic of Panama. These munitions are remnants from research, development, and testing conducted jointly by an American, British, and Canadian effort during, and shortly after, World War II. By a letter dated May 8, 2013, the Republic of Panama formally requested U.S. assistance and limited its request to disposing of only these eight U.S.-origin chemical munitions. This section also includes certain related conditions and a sunset date for the authorization.

Section 12xx—Modification and Extension of Authority to Conduct Activities to Enhance the Capability of Foreign Countries to Respond to Incidents Involving Weapons of Mass Destruction

This section would modify section 1204 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113-66) to include a 48-hour congressional notification when assistance expected to exceed \$4.0 million is provided to certain foreign countries, to cap the funds available at \$20.0 million, and extend the authority 1 year, through September 30, 2020.

TITLE XV—AUTHORIZATION OF ADDITIONAL APPROPRIATIONS FOR OVERSEAS CONTINGENCY OPERATIONS

LEGISLATIVE PROVISIONS

SUBTITLE D—LIMITATIONS, REPORTS, AND OTHER MATTERS

Section 15xx—Joint Improvised Explosive Device Defeat Fund

This section would modify subsection 1532(a) of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92) by extending the use and transfer authority for the Joint Improvised Explosive Device Defeat Fund to fiscal year 2017. This section would also modify section 1532(c) of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239) by expanding the foreign governments to whom assistance may be provided in order to counter the flow of improvised explosive device precursor chemicals. Finally, this section would extend the authority for interdiction of improvised explosive device precursor chemicals to December 31, 2017.

Section 15xx—Extension of Authority to Use Joint Improvised Explosive Device Defeat Fund for Training of Foreign Security Forces to Defeat Improvised Explosive Devices

This section would modify section 1533(e) of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92) by extending the Authority to Use the Joint Improvised Explosive Device Defeat Fund for Training of Foreign Security Forces to Defeat Improvised Explosive Devices and precursor chemicals from September 30, 2018, to September 30, 2020.

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE C—CYBERSPACE-RELATED MATTERS

Section 16xx—Special Emergency Procurement Authority to Facilitate the Defense Against or Recovery from a Cyber Attack

This section would modify the current special procurement authority in section 1903(a)(2) of title 41, United States Code, to include use of such authority for recovery from or defense against cyber attacks.

Section 16xx—Change in Name of National Defense University's Information Resources Management College to College of Information and Cyberspace

This section would modify section 2165 of title 10, United States Code, to change the name of the Information Resources Management College to the College of Information and Cyberspace.

Section 16xx—Requirement to Enter into Agreements Relating to Use of Cyber Opposition Forces

This section would require the Secretary of Defense to enter into agreements with each combatant command relating to the use of cyber opposition forces by September 30, 2017. This section would also require the development of a joint certification and training standard for cyber opposition forces by March 31, 2017.

The committee recognizes that the Department is making strides in establishing, manning, and training an adequate cyber mission force to help defend Department of Defense networks and information systems. An important aspect of that training, as well as the maintenance of long-term proficiency, will be through the use of cyber opposition forces that can realistically emulate the types of threat actors these teams will likely face. Just as conventional forces often face opposition forces in training exercises to improve their combat capability, the committee recognizes that such practices will have great utility in the cyber domain.

The committee also believes that the Department's move to a persistent training environment should be matched with the ability to continuously integrate such cyber opposition force training into these ongoing training evolutions. As the Department tries to marry the persistent training environment with continuous opposition force training, the committee believes that there will be a number of issues that should be addressed. In addition to the need to provide a joint training standard for those teams that mirrors the joint training standard for the cyber mission teams, the committee recognizes that special arrangements will be needed to deconflict training from real world activities that may happen on mission networks. The committee urges the Department to address these kinds of issues in developing agreements with the combatant commands to integrate cyber opposition force training into continuous and ongoing training activities.

Section 16xx—Limitation on Availability of Funds for Cryptographic Systems and Key Management Infrastructure

This section would limit the amount of authorized funds available to be obligated or expended in fiscal year 2017 for cryptographic systems and key management infrastructure until the Secretary of Defense, in coordination with the Director of the National Security Agency, provides a report on the integration of the cryptographic modernization and key management infrastructure programs of the military departments, including a description of how the military departments have implemented stronger leadership, increased integration, and reduced redundancy with respect to such modernization and programs.

BILL LANGUAGE

1 SEC. 1 **[Log 63805]. TERMINATION OF QUARTERLY RE-**
2 **PORING ON USE OF COMBAT MISSION RE-**
3 **QUIREMENTS FUNDS.**

4 Section 123(a)(1) of the Ike Skelton National De-
5 fense Authorization Act for Fiscal Year 2011 (Public Law
6 111-383; 124 Stat. 4158; 10 U.S.C. 167 note.) is amend-
7 ed by inserting “ending on or before September 30, 2018”
8 after “each fiscal quarter”.

1 SEC. 2 **[Log 62715]. LIMITATION ON AVAILABILITY OF**
2 **FUNDS FOR DEFENSE INNOVATION UNIT EX-**
3 **PERIMENTAL.**

4 (a) LIMITATION.—Of the funds specified in sub-
5 section (c), not more than 80 percent may be obligated
6 or expended until the date on which the Secretary of De-
7 fense submits to the congressional defense committees the
8 report under subsection (b).

9 (b) REPORT REQUIRED.—The Secretary of Defense
10 shall submit to the congressional defense committees a re-
11 port on the Defense Innovation Unit Experimental. Such
12 report shall include the following:

13 (1) The charter and mission statement of the
14 Unit.

15 (2) A description of—

16 (A) the governance structure of the Unit;
17 (B) the metrics used to measure the effec-
18 tiveness of the Unit;

19 (C) the process for coordinating and
20 deconflicting the activities of the Unit with
21 similar activities of the military departments,
22 Defense Agencies, and other departments and
23 agencies of the Federal Government, including
24 activities carried out by In-Q-Tel, the Defense

1 Advanced Research Projects Agency, and De-
2 partment of Defense laboratories;

3 (D) the direct staffing requirements of the
4 Unit, including a description of the desired
5 skills and expertise of such staff;

6 (E) the number of civilian and military
7 personnel provided by the military departments
8 and Defense Agencies to support the Unit;

9 (F) any planned expansion to new sites,
10 the metrics used to identify such sites, and an
11 explanation of how such expansion will provide
12 access to innovations of nontraditional defense
13 contractors (as such term is defined in section
14 2302 of title 10, United States Code) that are
15 not otherwise accessible;

16 (G) how compliance with Department of
17 Defense requirements could affect the ability of
18 such nontraditional defense contractors to mar-
19 ket products and obtain funding; and

20 (H) how to treat intellectual property that
21 has been developed with little or no government
22 funding.

23 (3) Any other information the Secretary deter-
24 mines to be appropriate.

1 (c) FUNDS SPECIFIED.—The funds specified in this
2 subsection are as follows:

3 (1) Funds authorized to be appropriated by this
4 Act or otherwise made available for fiscal year 2017
5 for operation and maintenance, Defense-wide, for
6 the Defense Innovation Unit Experimental.

7 (2) Funds authorized to be appropriated by this
8 Act or otherwise made available for fiscal year 2017
9 for research, development, test, and evaluation, De-
10 fense-wide, for the Defense Innovation Unit Experi-
11 mental.

1 SEC. 2 **[Log 62738]. PROHIBITION ON AVAILABILITY OF**
2 **FUNDS FOR COUNTERING WEAPONS OF MASS**
3 **DESTRUCTION SYSTEM CONSTELLATION.**

4 (a) PROHIBITIONS.—None of the funds authorized to
5 be appropriated by this Act or otherwise made available
6 for fiscal year 2017 for the countering weapons of mass
7 destruction situational awareness information system com-
8 monly known as “Constellation” may be obligated or ex-
9 pended for research, development, or prototyping for such
10 system.

11 (b) REVIEW.—The Chief Information Officer of the
12 Department of Defense, in consultation with the Director
13 of the Defense Information Systems Agency, shall review
14 the requirements and program plan for research, develop-
15 ment, and prototyping for the Constellation system.

16 (c) REPORT REQUIRED.—Not later than February 1,
17 2017, the Chief Information Officer of the Department of
18 Defense, in consultation with the Director of the Defense
19 Information Systems Agency, shall submit to the congres-
20 sional defense committees a report on the review under
21 subsection (b). Such report shall include the following,
22 with respect to the Constellation system:

23 (1) A review of the major software components
24 of the system and an explanation of the require-

1 ments of the Department of Defense with respect to
2 each such component.

3 (2) Identification of elements and applications
4 of the system that cannot be implemented using the
5 existing technical infrastructure and tools of the De-
6 partment of Defense or the infrastructure and tools
7 in development.

8 (3) A description of major developmental mile-
9 stones and decision points for additional prototypes
10 needed to establish the full capabilities of the sys-
11 tem, including a timeline and detailed metrics and
12 criteria for each such milestone and decision point.

13 (4) An overview of a security plan to achieve an
14 accredited cross-domain solution system, including
15 security milestones and proposed security architec-
16 ture to mitigate both insider and outsider threats.

17 (5) Identification of the planned categories of
18 end-users of the system, linked to organizations,
19 mission requirements, and concept of operations, the
20 expected total number of end-users, and the associ-
21 ated permissions granted to such users.

22 (6) A cost estimate for the full life-cycle cost to
23 complete the Constellation system.

1 SEC. 2____.**[Log 62743] IMPROVED BIOSAFETY FOR HAN-**

2 **DLING OF SELECT AGENTS AND TOXINS.**

3 (a) **QUALITY CONTROL AND QUALITY ASSURANCE**
4 **PROGRAM.**—The Secretary of Defense, acting through the
5 executive agent for the biological select agent and toxin
6 biosafety program of the Department of Defense, shall
7 carry out a program to implement certain quality control
8 and quality assurance measures at each covered facility.

9 (b) **QUALITY CONTROL AND QUALITY ASSURANCE**
10 **MEASURES.**—Subject to subsection (c), the quality control
11 and quality assurance measures implemented at each cov-
12 ered facility under subsection (a) shall include the fol-
13 lowing:

14 (1) Designation of an external manager to over-
15 see quality assurance and quality control.

16 (2) Environmental sampling and inspection.

17 (3) Production procedures that prohibit oper-
18 ations where live biological select agents and toxins
19 are used in the same laboratory where viability test-
20 ing is conducted.

21 (4) Production procedures that prohibit work
22 on multiple organisms or multiple strains of one or-
23 ganism within the same biosafety cabinet.

1 (5) A video surveillance program that uses
2 video monitoring as a tool to improve laboratory
3 practices in accordance with regulatory require-
4 ments.

5 (6) Formal, recurring data reviews of produc-
6 tion in an effort to identify data trends and non-
7 conformance issues before such issues affect end
8 products.

9 (7) Validated protocols for production processes
10 to ensure that process deviations are adequately vet-
11 ted prior to implementation.

12 (8) Maintenance and calibration procedures and
13 schedules for all tools, equipment, and irradiators.

14 (c) WAIVER.—In carrying out the program under
15 subsection (a), the Secretary may waive any of the quality
16 control and quality assurance measures required under
17 subsection (b) in the interest of national defense.

18 (d) STUDY AND REPORT REQUIRED.—

19 (1) The Secretary of Defense shall carry out a
20 study to evaluate—

21 (A) the feasibility of consolidating covered
22 facilities within a unified command to minimize
23 risk;

24 (B) opportunities to partner with industry
25 for the production of biological select agents

1 and toxins and related services in lieu of main-
2 taining such capabilities within the Department
3 of the Army; and

4 (C) whether operations under the biological
5 select agent and toxin production program
6 should be transferred to another government or
7 commercial laboratory that may be better suited
8 to execute production for non-Department of
9 Defense customers.

10 (2) Not later than February 1, 2017, the Sec-
11 retary shall submit to the congressional defense com-
12 mittees a report on the results of the study under
13 paragraph (1).

14 (e) COMPTROLLER GENERAL REVIEW.—Not later
15 than September 1, 2017, the Comptroller General of the
16 United States shall submit to the congressional defense
17 committees a report that includes the following:

18 (1) A review of—

19 (A) the actions taken by the Department
20 of Defense to address the findings and rec-
21 ommendations of the report of the Department
22 of the Army titled “Individual and Institutional
23 Accountability for the Shipment of Viable Bacil-
24 lus Anthracis from Dugway Proving Grounds”,
25 dated December 15, 2015, including any ac-

1 tions taken to address the culture of compla-
2 cency in the biological select agent and toxin
3 production program identified in such report;
4 and

5 (B) the progress of the Secretary in car-
6 rying out the program under subsection (a).

7 (2) An analysis of the study and report under
8 subsection (d).

9 (f) DEFINITIONS.—In this section:

10 (1) The term “covered facility” means any fa-
11 cility of the Department of Defense that produces
12 biological select agents and toxins.

13 (2) The term “biological select agent and toxin”
14 means any agent or toxin identified under—

15 (A) section 331.3 of title 7, Code of Fed-
16 eral Regulations;

17 (B) section 121.3 or section 121.4 of title
18 9, Code of Federal Regulations; or

19 (C) section 73.3 or section 73.4 of title 42,
20 Code of Federal Regulations.

1 SEC. 2 **[Log 63123]. MODERNIZATION OF SECURITY**

2 **CLEARANCE INFORMATION TECHNOLOGY AR-**

3 **CHITECTURE.**

4 (a) IN GENERAL.—The Secretary of Defense, in con-
5 sultation with the Director of National Intelligence and
6 the Director of the Office of Personnel Management, shall
7 develop and implement an information technology system
8 (in this section referred to as the “System”) to—

9 (1) modernize and sustain the security clear-
10 ance information architecture of the National Back-
11 ground Investigations Bureau and the Department
12 of Defense;

13 (2) support decision-making processes for the
14 evaluation and granting of personnel security clear-
15 ances;

16 (3) improve cyber security capabilities with re-
17 spect to sensitive security clearance data and proc-
18 esses;

19 (4) reduce the complexity and cost of the secu-
20 rity clearance process;

21 (5) provide information to managers on the fi-
22 nancial and administrative costs of the security
23 clearance process;

1 (6) strengthen the ties between counterintelligence
2 and personnel security communities; and

3 (7) improve system standardization in the security
4 clearance process.

5 (b) GUIDANCE REQUIRED.—Not later than 180 days
6 after the date of the enactment of this Act, the Secretary
7 of Defense, in consultation with the Director of National
8 Intelligence and the Director of the Office of Personnel
9 Management, shall issue guidance establishing the respec-
10 tive roles, responsibilities, and obligations of the Secretary
11 and Directors with respect to the development and imple-
12 mentation of the System.

13 (c) ELEMENTS OF SYSTEM.—In developing the Sys-
14 tem under subsection (a), the Secretary shall—

15 (1) conduct a review of security clearance busi-
16 ness processes and, to the extent practicable, modify
17 such processes to maximize compatibility with the
18 security clearance information technology architec-
19 ture to minimize the need for customization of the
20 System;

21 (2) conduct business process mapping (as such
22 term is defined in section 2222(i) of title 10, United
23 States Code) of the business processes described in
24 paragraph (1);

1 (3) use spiral development and incremental ac-
2 quisition practices to rapidly deploy the System, in-
3 cluding through the use of prototyping and open ar-
4 chitecture principles;

5 (4) establish a process to identify and limit
6 interfaces with legacy systems and to limit
7 customization of any commercial information tech-
8 nology tools used;

9 (5) establish automated processes for meas-
10 uring the performance goals of the System; and

11 (6) incorporate capabilities for the continuous
12 monitoring of network security and the mitigation of
13 insider threats to the System.

14 (d) COMPLETION DATE.—The Secretary shall com-
15 plete the development and implementation of the System
16 by not later than September 30, 2019.

17 (e) BRIEFING.—Beginning on December 1, 2016,
18 and on a quarterly basis thereafter until the completion
19 date of the System under subsection (d), the Secretary of
20 Defense shall provide a briefing to the Committees on
21 Armed Services of the Senate and House of Representa-
22 tives (and other appropriate congressional committees on
23 request) on the progress of the Secretary in developing
24 and implementing the System.

1 (f) REVIEW OF APPLICABLE LAWS.—The Secretary
2 shall review laws, regulations, and executive orders relat-
3 ing to the maintenance of personnel security clearance in-
4 formation by the Federal Government. Not later than 90
5 days after the date of the enactment of this Act, the Sec-
6 retary shall provide to the Committees on Armed Services
7 of the Senate and House of Representatives (and other
8 appropriate congressional committees on request) a brief-
9 ing that includes—

10 (1) the results of the review; and
11 (2) recommendations, if any, for consolidating
12 and clarifying laws, regulations, and executive orders
13 relating to the maintenance of personnel security
14 clearance information by the Federal Government.

15 (g) APPROPRIATE CONGRESSIONAL COMMITTEES
16 DEFINED.—In this section, the term “appropriate con-
17 gressional committees” means—

18 (1) the Select Committee on Intelligence, the
19 Committee on Homeland Security and Governmental
20 Affairs, and the Committee on Appropriations of the
21 Senate; and

22 (2) the Permanent Select Committee on Intel-
23 ligence, the Committee on Oversight and Govern-
24 ment Reform, and the Committee on Appropriations
25 of the House of Representatives.

1 SEC. 2 **[Log 62714]. STRATEGY FOR ASSURED ACCESS TO**

2 **TRUSTED MICROELECTRONICS.**

3 (a) STRATEGY.—The Secretary of Defense shall de-
4 velop a strategy to ensure that the Department of Defense
5 has assured access to trusted microelectronics by not later
6 than September 30, 2020.

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

9 (1) Definitions of the various levels of trust re-
10 quired by classes of Department of Defense systems.

11 (2) Means of classifying systems of the Depart-
12 ment of Defense based on the level of trust such sys-
13 tems are required to maintain with respect to micro-
14 electronics.

15 (3) Means by which trust in microelectronics
16 can be assured.

17 (4) Means to increase the supplier base for as-
18 sured microelectronics to ensure multiple supply
19 pathways.

20 (5) An assessment of the microelectronics needs
21 of the Department of Defense in future years, in-
22 cluding the need for trusted, radiation-hardened
23 microelectronics.

1 (6) An assessment of the microelectronic needs
2 of the Department of Defense that may not be ful-
3 filled by entities outside the Department of Defense.

4 (7) The resources required to assure access to
5 trusted microelectronics, including infrastructure
6 and investments in science and technology.

7 (c) SUBMISSION.—Not later than one year after the
8 date of the enactment of this Act, the Secretary shall sub-
9 mit to the congressional defense committees the strategy
10 developed under subsection (a). The strategy shall be sub-
11 mitted be in unclassified form, but may include a classified
12 annex.

13 (d) DIRECTIVE REQUIRED.—Not later than Sep-
14 tember 30, 2020, the Secretary of Defense shall issue a
15 directive for the Department of Defense describing how
16 Department of Defense entities may access assured and
17 trusted microelectronics supply chains for Department of
18 Defense systems.

19 (e) CERTIFICATION.—Not later than September 30,
20 2020, the Secretary of the Defense shall certify to the con-
21 gressional defense committees that—

22 (1) the strategy developed under subsection (a)
23 has been implemented; and

24 (2) the Department of Defense has an assured
25 means for accessing a sufficient supply of trusted

1 microelectronics, as required by the strategy devel-
2 oped under subsection (a).

3 (f) DEFINITION.—In this section, the terms “trust”
4 and “trusted” refer, with respect to microelectronics, to
5 the ability of the Department of Defense to have con-
6 fidence that the microelectronics function as intended and
7 are free of exploitable vulnerabilities, either intentionally
8 or unintentionally designed or inserted as part of the sys-
9 tem at any time during its life cycle.

1 SEC. 2 **[Log 62724]. LABORATORY QUALITY ENHANCE-**
2 **MENT PROGRAM.**

3 (a) IN GENERAL.—The Secretary of Defense, acting
4 through the Assistant Secretary of Defense for Research
5 and Engineering, shall carry out a Program to be known
6 as the “Laboratory Quality Enhancement Program”
7 under which the Secretary shall establish the panels de-
8 scribed in subsection (b) and direct such panels—

9 (1) to review and make recommendations to the
10 Secretary with respect to—

11 (A) existing policies and practices affecting
12 the science and technology reinvention labora-
13 tories to improve the research output of such
14 laboratories; and

15 (B) new initiatives proposed by the science
16 and technology reinvention laboratories;

17 (2) to support implementation of current and
18 future initiatives affecting the science and tech-
19 nology reinvention laboratories; and

20 (3) to conduct assessments or data analysis on
21 such other issues as the Secretary determines to be
22 appropriate.

23 (b) PANELS.—The panels described in this subsection
24 are:

1 (1) A panel on personnel, workforce development,
2 and talent management.

3 (2) A panel on facilities and infrastructure.

4 (3) A panel on research strategy, technology
5 transfer, and industry partnerships.

6 (4) A panel on oversight, administrative, and
7 regulatory processes.

8 (c) COMPOSITION OF PANELS.—

9 (1) Each panel described in subsection (b) shall
10 be composed of not less than 4 members.

11 (2) Each panel described in paragraphs (1)
12 through (3) of subsection (b) shall be composed of
13 subject matter and technical management experts
14 from—

15 (A) laboratories and research centers of
16 the Army, Navy and Air Force;

17 (B) appropriate Defense Agencies;

18 (C) the Office of the Assistant Secretary of
19 Defense for Research and Engineering; and

20 (D) such other entities of the Department
21 of Defense as the Secretary determines to be
22 appropriate.

23 (3) The panel described in subsection (b)(4)
24 shall be composed of—

- 1 (A) the Director of the Army Research
2 Laboratory;
3 (B) the Director of the Air Force Research
4 Laboratory;
5 (C) the Director of the Naval Research
6 Laboratory; and
7 (D) such other members as the Secretary
8 determines to be appropriate.

9 (d) GOVERNANCE OF PANELS.—

10 (1) The chairperson of each panel shall be se-
11 lected by its members.

12 (2) The panel described in subsection (b)(4)
13 shall—

14 (A) oversee the activities of the panels de-
15 scribed in paragraphs (1) through (3) of sub-
16 section (c);

17 (B) determine the subject matter to be
18 considered by the panels; and

19 (C) provide the recommendations of the
20 panels to the Secretary.

21 (e) PERSONNEL DEMONSTRATION PROJECT AU-
22 THORITY.—Section 342(b) of the National Defense Au-
23 thorization Act for Fiscal Year 1995 (Public Law 103-
24 337; 108 Stat. 2721) (as amended by section
25 1114(a)(2)(C) of the National Defense Authorization Act

1 for Fiscal Year 2001 (Public Law 106-398; 114 Stat.
2 1654A-315)) is amended by adding at the end the fol-
3 lowing new paragraph:

4 “(4) In carrying out this subsection, the Sec-
5 retary shall act through the Assistant Secretary of
6 Defense for Research and Engineering.”.

7 (f) SCIENCE AND TECHNOLOGY REINVENTION LAB-
8 ORATORY DEFINED.—In this section, the term “science
9 and technology reinvention laboratory” means a science
10 and technology reinvention laboratory designated under
11 section 1105 of the National Defense Authorization Act
12 for Fiscal Year 2010 (Public Law 111-84; 10 U.S.C.
13 2358 note).

1 SEC. 2 **[Log 63124]. PILOT PROGRAM ON EVALUATION OF**

2 **COMMERCIAL INFORMATION TECHNOLOGY.**

3 (a) PILOT PROGRAM.—The Director of the Defense
4 Information Systems Agency shall carry out a pilot pro-
5 gram to evaluate commercially available information tech-
6 nology tools to better understand the potential impact of
7 such tools on networks and computing environments of the
8 Department of Defense.

9 (b) ACTIVITIES.—Activities under the pilot program
10 may include the following:

11 (1) Prototyping, experimentation, operational
12 demonstration, military user assessments, and other
13 means of obtaining quantitative and qualitative feed-
14 back on the commercial information technology
15 products.

16 (2) Engagement with the commercial informa-
17 tion technology industry to—

18 (A) forecast military requirements and
19 technology needs; and

20 (B) support the development of market
21 strategies and program requirements before fi-
22 nalizing acquisition decisions and strategies.

1 (3) Assessment of novel or innovative commer-
2 cial technology for use by the Department of De-
3 fense.

4 (4) Assessment of novel or innovative con-
5 tracting mechanisms to speed delivery of capabilities
6 to the Armed Forces.

7 (5) Solicitation of operational user input to
8 shape future information technology requirements of
9 the Department of Defense.

10 (c) LIMITATION ON AVAILABILITY OF FUNDS.—Of
11 the amounts authorized to be appropriated for research,
12 development, test, and evaluation, Defense-wide, for each
13 of fiscal years 2017 through 2022, not more than
14 \$15,000,000 may be expended on the pilot program in any
15 such fiscal year.

1 SEC. 2 **[Log 63566]. REPORT ON ELECTRONIC WARFARE**

2 **CAPABILITIES.**

3 (a) REPORT REQUIRED.—Not later than April 1,
4 2017, the Under Secretary of Defense for Acquisition,
5 Technology, and Logistics, acting through the Electronic
6 Warfare Executive Committee, shall submit to the con-
7 gressional defense committees a report on the electronic
8 warfare capabilities of the Department of Defense.

9 (b) ELEMENTS.—The report under subsection (a)
10 shall include the following:

11 (1) A strategy for advancing and accelerating
12 research, development, test, and evaluation, and
13 fielding, of electronic warfare capabilities to meet
14 current and projected requirements, including rec-
15 commendations for streamlining acquisition processes
16 with respect to such capabilities.

17 (2) A methodology for synchronizing and over-
18 seeing electronic warfare strategies, operational con-
19 cepts, and programs across the Department of De-
20 fense, including electronic warfare programs that
21 support or enable cyber operations.

22 (3) The training and operational support re-
23 quired for fielding and sustaining current and

1 planned investments in electronic warfare capabili-
2 ties.

3 (4) A comprehensive list of investments of the
4 Department of Defense in electronic warfare capa-
5 bilities, including the capabilities to be developed,
6 procured, or sustained in—

7 (A) the budget of the President for fiscal
8 year 2018 submitted to Congress under section
9 1105(a) of title 31, United States Code; and

10 (B) the future-years defense program sub-
11 mitted to Congress under section 221 of title
12 10, United States Code, for that fiscal year.

13 (5) Any other information the Secretary deter-
14 mines to be appropriate.

15 (c) FORM.—The report under subsection (a) shall be
16 submitted in unclassified form, but may include a classi-
17 fied annex.

1 SEC. 8 [Log 62758]. AMENDMENTS RELATED TO DETEC-
2 TION AND AVOIDANCE OF COUNTERFEIT
3 ELECTRONIC PARTS.

4 Section 818 of the National Defense Authorization
5 Act for Fiscal Year 2012 (Public Law 112–81; 10 U.S.C.
6 2302 note) is amended—

7 (1) in paragraph (3) of subsection (c)—
8 (A) by striking the heading and inserting
9 “SUPPLIERS MEETING ANTICOUNTERFEITING
10 REQUIREMENTS.—”;

11 (B) in subparagraph (A)(i), by striking
12 “trusted suppliers in accordance with regula-
13 tions issued pursuant to subparagraph (C) or
14 (D) who” and inserting “suppliers that meet
15 anticontroling requirements in accordance
16 with regulations issued pursuant to subpara-
17 graph (C) or (D) and that”;

18 (C) in subparagraphs (A)(ii) and (A)(iii),
19 by striking “trusted suppliers” each place it ap-
20 pears and inserting “suppliers that meet
21 anticontroling requirements”;

22 (D) in subparagraph (C), by striking “as
23 trusted suppliers those” and inserting “sup-
24 pliers”;

1 SEC. 8 [Log 63632]. REVIEW OF ANTI-COMPETITIVE
2 SPECIFICATIONS IN INFORMATION TECH-
3 NOLOGY ACQUISITIONS.

4 (a) REVIEW REQUIRED.—Not later than 180 days
5 after the date of the enactment of this Act, the Under
6 Secretary of Defense for Acquisition, Technology, and Lo-
7 gistics shall conduct a review of the policy, guidance, regu-
8 lations, and training related to specifications included in
9 information technology acquisitions to ensure current poli-
10 cies eliminate the unjustified use of potentially anti-com-
11 petitive specifications. In conducting the review, the Under
12 Secretary shall examine the use of brand names or propri-
13 etary specifications or standards in solicitations for pro-
14 curements of goods and services, as well as the current
15 acquisition training curriculum related to those areas.

16 (b) BRIEFING REQUIRED.—Not later than 270 days
17 after the date of the enactment of this Act, the Under
18 Secretary shall provide a briefing to the Committees on
19 Armed Services of the Senate and House of Representa-
20 tives on the results of the review required by subsection
21 (a).

22 (c) ADDITIONAL GUIDANCE.—Not later than one
23 year after the date of the enactment of this Act, the Under
24 Secretary shall revise policies, guidance, and training to

- 1 incorporate such recommendations as the Under Secretary
- 2 considers appropriate from the review required by sub-
- 3 section (a).

1 SEC. 10 [Log 63419]. MATTERS FOR INCLUSION IN RE-
2 **PORT ON DESIGNATION OF COUNTRIES FOR**
3 **WHICH REWARDS MAY BE PAID UNDER DE-**
4 **PARTMENT OF DEFENSE REWARDS PRO-**
5 **GRAM.**

6 Section 127b(h) of title 10, United States Code, is
7 amended—

8 (1) in paragraph (2), by inserting “and jus-
9 tification” after “reason”; and

10 (2) by amending paragraph (3) to read as fol-
11 lows:

12 “(3) An estimate of the amount or value of the
13 rewards to be paid as monetary payment or pay-
14 ment-in-kind under this section.”.

1 SEC. 10 [Log 63806]. FREQUENCY OF COUNTERTER-
2 RORISM OPERATIONS BRIEFINGS.

3 (a) IN GENERAL.—Subsection (a) of section 485 of
4 title 10, United States Code is amended by striking “quar-
5 terly” and inserting “monthly”.

6 (b) SECTION HEADING.—The section heading for
7 such section is amended by striking “**Quarterly**” and
8 inserting “**Monthly**”.

9 (c) CLERICAL AMENDMENT.—The table of sections
10 at the beginning of chapter 23 of such title is amended
11 by striking the item relating to section 485 and inserting
12 the following new item:

“485. Monthly counterterrorism operations briefings.”.

1 SEC. 10 [Log 62742]. CONGRESSIONAL NOTIFICATION OF
2 BIOLOGICAL SELECT AGENT AND TOXIN
3 THEFT, LOSS, OR RELEASE INVOLVING THE
4 DEPARTMENT OF DEFENSE.

5 (a) NOTIFICATION REQUIREMENT.—Not later than
6 15 days after notice of any theft, loss, or release of a bio-
7 logical select agent or toxin involving the Department of
8 Defense is provided to the Centers for Disease Control and
9 Prevention or the Animal and Plant Health Inspection
10 Service, as specified by section 331.19 of part 7 of the
11 Code of Federal Regulations, the Secretary of Defense
12 shall provide to the congressional defense committees no-
13 tice of such theft, loss, or release.

14 (b) ELEMENTS.—Notice of a theft, loss, or release
15 of a biological select agent or toxin under subsection (a)
16 shall include each of the following:

17 (1) The name of the agent or toxin and any
18 identifying information, including the strain or other
19 relevant characterization information.

20 (2) An estimate of the quantity of the agent or
21 toxin stolen, lost, or released.

22 (3) The location or facility from which the
23 theft, loss, or release occurred.

- 1 (4) In the case of a release, any hazards posed
- 2 by the release and the number of individuals poten-
- 3 tially exposed to the agent or toxin.
- 4 (5) Actions taken to respond to the theft, loss,
- 5 or release.

1 SEC. 10 [Log 62805]. REPORT ON SERVICE-PROVIDED
2 SUPPORT TO UNITED STATES SPECIAL OPER-
3 ATIONS FORCES.

4 (a) REPORT REQUIRED.—Not later than 180 days
5 after the date of the enactment of this Act, the Secretary
6 of Defense shall submit to the congressional defense com-
7 mittees a written report on common service support con-
8 tributed from each of the military services toward special
9 operations forces. Such report shall include—

10 (1) detailed information about the resources al-
11 located by each military service for combat support,
12 combat service support, and base operating support
13 for special operations forces; and

14 (2) an assessment of the specific effects that fu-
15 ture manpower and force structure changes are like-
16 ly to have on the capability of each of the military
17 services to provide common service support to special
18 operations forces.

19 (b) ANNUAL UPDATES.—For each of fiscal years
20 2018 through 2020, the Secretary of Defense shall submit
21 to the congressional defense committees an update to the
22 report required under subsection (a).

23 (c) FORM OF REPORT.—The report required under
24 subsection (a) and each update provided under subsection

- 1 (b) shall be submitted in unclassified form, but may contain a classified annex.
- 2

1 SEC. 10 [Log 62744]. NATIONAL BIODEFENSE STRATEGY.

2 (a) STRATEGY AND IMPLEMENTATION PLAN RE-
3 QUIRED.—The Secretary of Defense, the Secretary of
4 Health and Human Services, the Secretary of Homeland
5 Security, and the Secretary of Agriculture shall jointly de-
6 velop a national biodefense strategy and associated imple-
7 mentation plan, which shall include a review and assess-
8 ment of biodefense policies, practices, programs and initia-
9 tives. Such Secretaries shall review and, as appropriate,
10 revise the strategy biennially.

11 (b) ELEMENTS.—The strategy and associated imple-
12 mentation plan required under subsection (a) shall include
13 each of the following:

14 (1) An inventory and assessment of all existing
15 strategies, plans, policies, laws, and interagency
16 agreements related to biodefense, including preven-
17 tion, deterrence, preparedness, detection, response,
18 attribution, recovery, and mitigation.

19 (2) A description of the biological threats, in-
20 cluding biological warfare, bioterrorism, naturally oc-
21 curring infectious diseases, and accidental exposures.

22 (3) A description of the current programs, ef-
23 forts, or activities of the United States Government
24 with respect to preventing the acquisition, prolifera-

1 tion, and use of a biological weapon, preventing an
2 accidental or naturally occurring biological outbreak,
3 and mitigating the effects of a biological epidemic.

4 (4) A description of the roles and responsibilities
5 of the Executive Agencies, including internal
6 and external coordination procedures, in identifying
7 and sharing information related to, warning of, and
8 protection against, acts of terrorism using biological
9 agents and weapons and accidental or naturally oc-
10 curring biological outbreaks.

11 (5) An articulation of related or required inter-
12 agency capabilities and whole-of-Government activi-
13 ties required to support the national biodefense
14 strategy.

15 (6) Recommendations for strengthening and im-
16 proving the current biodefense capabilities, authori-
17 ties, and command structures of the United States
18 Government.

19 (7) Recommendations for improving and for-
20 malizing interagency coordination and support mech-
21 anisms with respect to providing a robust national
22 biodefense.

23 (8) Any other matters the Secretary of Defense,
24 the Secretary of Health and Human Services, the

1 Secretary of Homeland Security, and the Secretary
2 of Agriculture determine necessary.

3 (c) SUBMITTAL TO CONGRESS.—Not later than 275
4 days after the date of the enactment of this Act, the Sec-
5 retary of Defense, the Secretary of Health and Human
6 Services, the Secretary of Homeland Security, and the
7 Secretary of Agriculture shall submit to the appropriate
8 congressional committees the strategy and associated im-
9 plementation plan required by subsection (a). The strategy
10 and implementation plan shall be submitted in unclassified
11 form, but may include a classified annex.

12 (d) BRIEFINGS.—Not later than March 1, 2017, and
13 annually thereafter until March 1, 2019, the Secretary of
14 Defense, the Secretary of Health and Human Services, the
15 Secretary of Homeland Security, and the Secretary of Ag-
16 riculture shall provide to the Committee on Armed Serv-
17 ices of the House of Representatives, the Committee on
18 Energy and Commerce of the House of Representatives,
19 the Committee on Homeland Security of the House of
20 Representatives, and the Committee on Agriculture of the
21 House of Representatives a joint briefing on the strategy
22 developed under subsection (a) and the status of the im-
23 plementation of such strategy.

24 (e) GAO REVIEW.—Not later than 180 days after the
25 date of the submittal of the strategy and implementation

1 plan under subsection (c), the Comptroller General of the
2 United States shall conduct a review of the strategy and
3 implementation plan to analyze gaps and resources
4 mapped against the requirements of the National Bio-
5 defense Strategy and existing United States biodefense
6 policy documents.

7 (f) APPROPRIATE CONGRESSIONAL COMMITTEES DE-
8 FINED.—In this section, the term “appropriate congres-
9 sional committees” means the following:

10 (1) The congressional defense committees.
11 (2) The Committee on Energy and Commerce
12 of the House of Representatives and the Committee
13 on Health, Education, Labor, and Pensions of the
14 Senate.

15 (3) The Committee on Homeland Security of
16 the House of Representatives and the Committee on
17 Homeland Security and Governmental Affairs of the
18 Senate.

19 (4) The Committee on Agriculture of the House
20 of Representatives and the Committee on Agri-
culture, Nutrition, and Forestry of the Senate.

1 SEC. 10 [Log 63692]. REPORT ON COUNTERPROLIFERA-
2 TION ACTIVITIES AND PROGRAMS.

3 (a) IN GENERAL.—The Secretary of Defense shall
4 submit to the congressional defense committees a biennial
5 report on the counterproliferation activities and programs
6 of the Department of Defense. The Secretary shall submit
7 the first such report by not later than May 1, 2017.

8 (b) MATTERS INCLUDED.—Each report required
9 under subsection (a) shall include each of the following:

10 (1) A complete list and assessment of existing
11 and proposed capabilities and technologies for sup-
12 port of United States nonproliferation policy and
13 counterproliferation policy, with regard to—

14 (A) interdiction;

15 (B) elimination;

16 (C) threat reduction cooperation;

17 (D) passive defenses;

18 (E) security cooperation and partner ac-
19 tivities;

20 (F) offensive operations;

21 (G) active defenses; and

22 (H) weapons of mass destruction con-
23 sequence management.

1 (2) For the existing and proposed capabilities
2 and technologies identified under paragraph (1), an
3 identification of goals, a description of ongoing ef-
4 forts, and recommendations for further enhance-
5 ments.

6 (3) A complete description of requirements and
7 priorities for the development and deployment of
8 highly effective capabilities and technologies, includ-
9 ing identifying areas for capability enhancement and
10 deficiencies in existing capabilities and technologies.

11 (4) A comprehensive discussion of the near-
12 term, mid-term, and long-term programmatic op-
13 tions for meeting requirements and eliminating defi-
14 ciencies, including the annual funding requirements
15 and completion dates established for each such op-
16 tion.

17 (5) An outline of interagency activities and ini-
18 tiatives.

19 (6) Any other matters the Secretary considers
20 appropriate.

21 (c) FORMS OF REPORT.—Each report under sub-
22 section (a) shall be submitted in unclassified form, but
23 may contain a classified annex.

1 (d) TERMINATION OF REQUIREMENT.—No report
2 shall be required to be submitted under this section after
3 January 31, 2021.

1 SEC. __. [LOG 63708] TWO-YEAR EXTENSION AND MODIFICA-
2 TION OF AUTHORIZATION OF NON-CONVEN-
3 TIONAL ASSISTED RECOVERY CAPABILITIES.

4 (a) EXTENSION OF AUTHORITY.—Subsection (h) of
5 section 943 of the Duncan Hunter National Defense Au-
6 thorization Act for Fiscal Year 2009 (Public Law 110–
7 417; 122 Stat. 4579), as most recently amended by sec-
8 tion 1271 of the National Defense Authorization Act for
9 Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1075),
10 is further amended by striking “2018” and inserting
11 “2020”.

12 (b) MODIFICATION TO AUTHORIZED ACTIVITIES.—
13 Subsection (c) of such section is amended by inserting “,
14 or other individuals, as determined by the Secretary of De-
15 fense, with respect to already established non-conventional
16 assisted recovery capabilities” before the period at the end
17 of the first sentence.

1 SEC. __. [LOG 62752] EXTENSION OF AUTHORITY FOR SUP-
2 PORT OF SPECIAL OPERATIONS TO COMBAT
3 TERRORISM.

4 Subsection (h) of section 1208 of the Ronald W.
5 Reagan National Defense Authorization Act for Fiscal
6 Year 2005 (Public Law 108–375; 118 Stat. 2086), as
7 most recently amended by section 1208(b) of the Carl
8 Levin and Howard P. “Buck” McKeon National Defense
9 Authorization Act for Fiscal Year 2015 (Public Law 113–
10 291; 128 Stat. 3541), is further amended by striking
11 “2017” and inserting “2020”.

1 SEC. __. [LOG 63122] AUTHORITY TO DESTROY CERTAIN
2 SPECIFIED WORLD WAR II-ERA UNITED
3 STATES-ORIGIN CHEMICAL MUNITIONS LO-
4 CATED ON SAN JOSE ISLAND, REPUBLIC OF
5 PANAMA.

6 (a) AUTHORITY.—

7 (1) IN GENERAL.—Subject to subsection (b),
8 the Secretary of Defense may destroy the chemical
9 munitions described in subsection (c).

10 (2) EX GRATIA ACTION.—The action authorized
11 by this section is “ex gratia” on the part of the
12 United States, as the term “ex gratia” is used in
13 section 321 of the Strom Thurmond National De-
14 fense Authorization Act for Fiscal Year 1999 (Pub-
15 lic Law 105–261; 10 U.S.C. 2701 note).

16 (3) CONSULTATION BETWEEN SECRETARY OF
17 DEFENSE AND SECRETARY OF STATE.—The Sec-
18 retary of Defense and the Secretary of State shall
19 consult and develop any arrangements with the Re-
20 public of Panama with respect to this section.

21 (b) CONDITIONS.—The Secretary of Defense may ex-
22 ercise the authority under subsection (a) only if the Re-
23 public of Panama has—

1 (1) revised the declaration of the Republic of
2 Panama under the Convention on the Prohibition of
3 the Development, Production, Stockpiling and Use
4 of Chemical Weapons and on Their Destruction to
5 indicate that the chemical munitions described in
6 subsection (c) are “old chemical weapons” rather
7 than “abandoned chemical weapons”; and

8 (2) affirmed, in writing, that it understands (A)
9 that the United States intends only to destroy the
10 munitions described in subsections (c) and (d), and
11 (B) that the United States is not legally obligated
12 and does not intend to destroy any other munitions,
13 munitions constituents, and associated debris that
14 may be located on San Jose Island as a result of re-
15 search, development, and testing activities conducted
16 on San Jose Island during the period of 1943
17 through 1947.

18 (c) CHEMICAL MUNITIONS.—The chemical munitions
19 described in this subsection are the eight United States-
20 origin chemical munitions located on San Jose Island, Re-
21 public of Panama, that were identified in the 2002 Final
22 Inspection Report of the Technical Secretariat of the Or-
23 ganization for the Prohibition of Chemical Weapons.

24 (d) LIMITED INCIDENTAL AUTHORITY TO DESTROY
25 OTHER MUNITIONS.—In exercising the authority under

1 subsection (a), the Secretary of Defense may destroy other
2 munitions located on San Jose Island, Republic of Pan-
3 ama, but only to the extent essential and required to reach
4 and destroy the chemical munitions described in sub-
5 section (c).

6 (e) SOURCE OF FUNDS.—Of the amounts authorized
7 to be appropriated by this Act, the Secretary of Defense
8 may use up to \$30,000,000 from amounts made available
9 for Chemical Agents and Munitions Destruction, Defense
10 to carry out the authority in subsection (a).

11 (f) SUNSET.—The authority under subsection (a)
12 shall terminate on the date that is three years after the
13 date of the enactment of this Act.

1 SEC. __. [LOG 63349] MODIFICATION AND EXTENSION OF
2 AUTHORITY TO CONDUCT ACTIVITIES TO EN-
3 HANCE THE CAPABILITY OF FOREIGN COUN-
4 TRIES TO RESPOND TO INCIDENTS INVOLV-
5 ING WEAPONS OF MASS DESTRUCTION.

6 (a) LIMITATION ON AVAILABILITY OF AUTHORITY
7 FOR OTHER COUNTRIES.—Subsection (b) of section 1204
8 of the National Defense Authorization Act for Fiscal Year
9 2014 (Public Law 113–66; 127 Stat. 896; 10 U.S.C. 401
10 note) is amended by striking “of the Secretary’s inten-
11 tion” and inserting “not later than 48 hours after the Sec-
12 retary makes a determination”.

13 (b) AVAILABILITY OF FUNDS.—Subsection (d)(1) of
14 such section is amended to read as follows:

15 “(1) FUNDS AVAILABLE.—Of the funds author-
16 ized to be appropriated for the Department of De-
17 fense for Operation and Maintenance, Defense-wide,
18 and available for the Defense Threat Reduction
19 Agency for a fiscal year, not more than \$20,000,000
20 may be made available for assistance under this sec-
21 tion for such fiscal year.”.

22 (c) NOTICE TO CONGRESS ON CERTAIN ASSIST-
23 ANCE.—Subsection (e) of such section, as amended by sec-
24 tion 1202 of the Carl Levin and Howard P. “Buck”

1 McKeon National Defense Authorization Act for Fiscal
2 Year 2015 (Public Law 113–291; 128 Stat. 3530), is fur-
3 ther amended—

4 (1) by striking “If the amount” and inserting
5 “If the Secretary of Defense determines that the
6 amount”;

7 (2) by striking “the Secretary of Defense shall
8 notify” and inserting “the Secretary shall notify”;
9 and

10 (3) by striking “of that fact” and inserting “of
11 such determination not later than 48 hours after
12 making the determination”.

13 (d) EXPIRATION.—Subsection (h) of such section, as
14 amended by section 1273 of the National Defense Author-
15 ization Act for Fiscal Year 2016 (Public Law 114–92; 129
16 Stat. 1076), is further amended by striking “September
17 30, 2019” and inserting “September 30, 2020”.

18 (e) EFFECTIVE DATE.—The amendments made by
19 this section take effect on the date of the enactment of
20 this Act and apply with respect to assistance authorized
21 to be provided under subsection (a) of section 1204 of the
22 National Defense Authorization Act for Fiscal Year 2014
23 on or after such date of enactment.

1 SEC. 15. [Log 62763]. JOINT IMPROVISED EXPLOSIVE DE-

2 VICE DEFEAT FUND.

3 (a) USE AND TRANSFER OF FUNDS.—Subsection
4 1532(a) of the National Defense Authorization Act for
5 Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1091)
6 is amended by striking “fiscal year 2016” and inserting
7 “fiscal years 2016 and 2017”.

8 (b) EXTENSION OF INTERDICTION OF IMPROVISED
9 EXPLOSIVE DEVICE PRECURSOR CHEMICALS AUTHOR-
10 ITY.—Section 1532(c) of the National Defense Authoriza-
11 tion Act for Fiscal Year 2013 (Public Law 112–239; 126
12 Stat. 2057) is amended—

13 (1) in paragraph (1)—

14 (A) by striking “for fiscal year 2013 and
15 for fiscal year 2016,” and inserting “for fiscal
16 years 2013, 2016, and 2017”;

17 (B) by inserting “with the concurrence of
18 the Secretary of State” after “may be available
19 to the Secretary of Defense”;

20 (C) by striking “of the Government of
21 Pakistan” and inserting “of foreign govern-
22 ments”; and

23 (D) by striking “from Pakistan to loca-
24 tions in Afghanistan”;

1 (2) in paragraph (2), by striking “of the Gov-
2 ernment of Pakistan” and inserting “of foreign gov-
3 ernments”;

4 (3) in paragraph (3)—

5 (A) in the matter preceding subparagraph
6 (A), by striking “the congressional defense com-
7 mittees” and inserting “Congress”; and

8 (B) in subparagraph (B)—

9 (i) by striking “the Government of
10 Pakistan” and inserting “foreign govern-
11 ments”; and

12 (ii) by striking “from Pakistan to lo-
13 cations in Afghanistan”; and

14 (4) in paragraph (4), as most recently amended
15 by section 1532(b)(2) of the National Defense Au-
16 thorization Act for Fiscal Year 2016 (Public Law
17 114–92; 129 Stat. 1091), by striking “December 31,
18 2016” and inserting “December 31, 2017”.

1 SEC. 15 [Log 62764]. EXTENSION OF AUTHORITY TO USE
2 JOINT IMPROVISED EXPLOSIVE DEVICE DE-
3 FEAT FUND FOR TRAINING OF FOREIGN SE-
4 CURITY FORCES TO DEFEAT IMPROVISED EX-
5 PLOSIVE DEVICES.

6 Section 1533(e) of the National Defense Authoriza-
7 tion Act for Fiscal Year 2016 (Public Law 114–92; 129
8 Stat. 1093) is amended by striking “September 30, 2018”
9 and inserting “September 30, 2020”.

1 SEC. 16 [Log 62718]. SPECIAL EMERGENCY PROCUREMENT
2 AUTHORITY TO FACILITATE THE DEFENSE AGAINST OR RECOVERY FROM A
3 CYBER ATTACK.

5 Section 1903(a)(2) of title 41, United States Code,
6 is amended by inserting “cyber,” before “nuclear.”.

1 SEC. 16 [Log 63121]. CHANGE IN NAME OF NATIONAL DE-
2 FENSE UNIVERSITY'S INFORMATION RE-
3 SOURCES MANAGEMENT COLLEGE TO COL-
4 LEGE OF INFORMATION AND CYBERSPACE.

5 Section 2165(b)(5) of title 10, United States Code,
6 is amended by striking “Information Resources Manage-
7 ment College” and inserting “College of Information and
8 Cyberspace”.

1 SEC. 16 [Log 63500]. REQUIREMENT TO ENTER INTO
2 AGREEMENTS RELATING TO USE OF CYBER
3 OPPOSITION FORCES.

4 (a) REQUIREMENT FOR AGREEMENTS.—Not later
5 than September 30, 2017, the Secretary of Defense shall
6 enter into an agreement with each combatant command
7 relating to the use of cyber opposition forces. Each agree-
8 ment shall require the command—

9 (1) to support a high state of mission readiness
10 in the command through the use of one or more
11 cyber opposition forces in continuous exercises and
12 other training activities as considered appropriate by
13 the commander of the command; and

14 (2) in conducting such exercises and training
15 activities, meet the standard required under sub-
16 section (b).

17 (b) JOINT STANDARD FOR CYBER OPPOSITION
18 FORCES.—Not later than March 31, 2017, the Secretary
19 of Defense shall issue a joint training and certification
20 standard for use by all cyber opposition forces within the
21 Department of Defense.

22 (c) BRIEFING REQUIRED.—Not later than September
23 30, 2017, the Secretary of Defense shall provide to the
24 congressional defense committees a briefing on—

1 (1) a list of each combatant command that has
2 entered into an agreement required by subsection
3 (a);

4 (2) with respect to each such agreement—

12 (C) identification of cyber opposition forces
13 trained and certified to operate at the joint
14 standard, as issued under subsection (b);

(D) identification of the annual exercises
that will include participation of the cyber oppo-
sition forces;

18 (E) identification of any shortfalls in re-
19 sources that may prevent annual exercises using
20 cyber opposition forces; and

1 SEC. 16. **[Log 63715] LIMITATION ON AVAILABILITY OF**
2 **FUNDS FOR CRYPTOGRAPHIC SYSTEMS AND**
3 **KEY MANAGEMENT INFRASTRUCTURE.**

4 (a) LIMITATION.—Of the funds authorized to be ap-
5 propriated by this Act or otherwise made available for fis-
6 cal year 2017 for cryptographic systems and key manage-
7 ment infrastructure, not more than 75 percent may be ob-
8 ligated or expended until the date on which the Secretary
9 of Defense, in consultation with the Director of the Na-
10 tional Security Agency, submits to the appropriate con-
11 gressional committees a report on the integration of the
12 cryptographic modernization and key management infra-
13 structure programs of the military departments, including
14 a description of how the military departments have imple-
15 mented stronger leadership, increased integration, and re-
16 duced redundancy with respect to such modernization and
17 programs.

18 (b) APPROPRIATE CONGRESSIONAL COMMITTEES
19 DEFINED.—In this section, the term “appropriate con-
20 gressional committees” means the following:

- 21 (1) The congressional defense committees.
22 (2) The Permanent Select Committee on Intel-
23 ligence of the House of Representatives.

DIRECTIVE REPORT LANGUAGE

Table Of Contents

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE I—PROCUREMENT

OTHER PROCUREMENT, ARMY

Items of Special Interest

Chemical, Biological, Radiological, and Nuclear Response Enterprise Information Management System

PROCUREMENT, MARINE CORPS

Items of Special Interest

Non-lethal ocular interruption capabilities

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, AIR FORCE

Items of Special Interest

Air Force directed energy initiatives

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

Items of Special Interest

Broad-spectrum antiviral drug modeling

Comptroller General review of commercial practices for trust in microelectronics

Counter-unmanned aerial systems roadmap

Department of Defense medical countermeasures Advanced Development and Manufacturing facility roadmap

Desalination technology

Human systems integration activities

Incentives for increasing private sector medical countermeasures development

MQ-9 anti-icing capability

Prioritization of joint test activities

Technology enablers for directed energy weapon systems

U.S. Special Operations Command rapid prototyping and SOFWERX initiative

OPERATIONAL TEST AND EVALUATION, DEFENSE

Items of Special Interest

Range capabilities for emerging advanced technologies

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

ITEMS OF SPECIAL INTEREST

Human Capital Plan for Business Transformation

TITLE X—GENERAL PROVISIONS

ITEMS OF SPECIAL INTEREST

OTHER MATTERS

Comptroller General Assessment of Deployable Identity Management Forensics Capability

Department of Defense Strategy for Countering Unconventional Warfare
Wassenaar Arrangement Impacts to the Department of Defense

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

ITEMS OF SPECIAL INTEREST

- Countering Adversarial Messaging
- Reporting Requirements of Authority for Support of Special Operations to Combat Terrorism
- Social Media Analytics and Publicly Available Information Supporting Battlespace Awareness
- Strategy for Regional Counter-Narrative Capabilities

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

ITEMS OF SPECIAL INTEREST

- Assessment of Department of Defense Efforts to Secure Internet of Things Cloud Access Points
- Comptroller General Assessment of the Management and Measurement of Cyber Activities
- Cyber Training Equivalency
- Host Based Security System Best Practices
- Information Assurance of Joint Test and Evaluation Activities
- Insider Threat Capabilities for the Joint Information Environment
- Strategic Plan for the Defense Insider Threat Management and Analysis Center

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE I—PROCUREMENT

OTHER PROCUREMENT, ARMY

Items of Special Interest

Chemical, Biological, Radiological, and Nuclear Response Enterprise Information Management System

The committee is aware that the National Guard Bureau Weapons of Mass Destruction-Civil Support Teams (CST) currently field a system, the CST Information Management System (CIMS), to provide a common operating picture, promote information sharing and real-time collaboration in an emergency situation, and support the CST mission of assisting and advising first responders and facilitating communications with other Federal resources. The committee is also aware that the CIMS system is being modified to establish an enterprise-capable tool, referred to as the National Guard Chemical, Biological, Radiological, and Nuclear Response Enterprise Information Management System 2018+ (NG CIMS 2018+), that will expand the capabilities of the CIMS to support the 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 believes it is important that this enhanced CIMS capability be fielded quickly and efficiently by utilizing prior investments to expand and enhance communication capability. The committee is aware of the plan to develop and establish the NG CIMS 2018+ through a multi-phase approach, including establishing initial operational capability in fiscal year 2016 and proving full operational capability in fiscal year 2018. Therefore, the committee directs the Secretary of Defense to provide a briefing to the Committee on Armed Services of the House of Representatives by December 1, 2016, detailing the status of the development of the NG CIMS 2018+ tool to date, as well as a description of the progress on providing the initial operational capability and an update on the future plans and milestones to establishment of full operational capability.

PROCUREMENT, MARINE CORPS

Items of Special Interest

Non-lethal ocular interruption capabilities

The committee continues to support the Department's efforts for accelerated development, fielding, and deployment of non-lethal technologies for both force application and force protection missions. The committee is encouraged by the Marine Corps' efforts to modernize and procure hail and warning, laser dazzlers, and other escalation of force systems. The committee recognizes that these materiel solutions allow personnel engaged in combat, stability and support, security, and force protection operations to employ visual technologies to non-lethally intercept and interdict personnel at safe standoff distances. These solutions provide commanders with a non-lethal hailing and warning capability applicable across the range of military operations to support Marine Corps missions when the minimization of civilian casualties and collateral damage is essential to mission success. The committee is concerned that the funding reductions over the past few years to both the Department's Non-Lethal Weapons program, and the services' procurements for non-lethal systems, will not be able to support the readiness need for escalation of force capabilities that may be needed for humanitarian relief efforts, non-combatant evacuation operations, and peacekeeping. The committee, therefore, directs the Secretary of the Navy to provide a briefing to the House Committee on Armed Services by November 1, 2016, on actions being taken to ensure sufficient procurement of such equipment to meet projected operational needs. This briefing should include details on the programming, planning, and budgeting for procurement of hail and warning, and other escalation of force systems.

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, AIR FORCE

Items of Special Interest

Air Force directed energy initiatives

The committee is aware that the Department of the Air Force established a Directed Energy Weapons (DEW) Integrated Product Team (IPT) in March 2016 to focus on operationalizing directed energy (DE) technologies. In addition to addressing technology development risks through science and technology efforts, the IPT will focus on policy issues, establishment of kinetic concepts of operation, opportunities for prototypes and experimentation, limitations, constraints, transition milestones, and critical decision points for Air Force strategic investment from 2016 to 2036. In addition, the DEW IPT will identify required test capabilities and acquisition infrastructure to support operationalizing DE. This information will be formalized in an Air Force DE Flight Plan.

The committee supports the effort to operationalize DE and recognizes the challenges, specifically the integration of DE on airborne platforms and resolution of policy issues, in achieving this goal. The committee understands that in producing the Air Force DE Flight Plan, initial concepts may prove unfeasible or not conducive to the overall Air Force Strategic Plan. Therefore, the committee directs the Secretary of the Air Force to provide a briefing to the House Committee on Armed Services by July 15, 2016, on the establishment of the IPT and efforts and progress to date. The briefing should include a discussion of any DE requirements as identified by U.S. Air Force Special Operations Command, including any AC-130 gunship requirements, such as those included in the unfunded priorities list submitted to the committee. Finally, the committee expects to be provided a copy of the Air Force DE Flight Plan upon its completion in October 2016.

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

Items of Special Interest

Broad-spectrum antiviral drug modeling

The committee understands the importance of developing efficient and effective countermeasures against a growing list of lethal pathogens, many of which have different variants. The committee is supportive of efforts to develop broad-spectrum antiviral drugs that can be used against many different pathogen threats. The committee further believes that rapid development of these drugs can be improved by using modeling software of the drug/virus interaction to perform high throughput screening of potential candidate drugs, leading to decreased development time. After candidate drugs have been identified, it is also important to establish partnerships with biosafety level 4 facilities to allow testing of the efficacy of these drugs. The committee understands that partnerships with not-for-profit 501C3 applied research facilities can provide unique capabilities and expertise throughout the drug development process.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by September 30, 2016, on the current and planned use of drug/virus interaction modeling software for high throughput screening of potential small molecule drugs. The briefing should also include a list of the current and potential partnerships with not-for-profit 501C3 applied research facilities, and the potential for partnerships between these 501C3 applied research facilities and the Department of Defense Advanced Development and Manufacturing facility.

Comptroller General review of commercial practices for trust in microelectronics

The committee remains concerned with the Department of Defense's ability to ensure access to cutting-edge microelectronics with the requisite level of verifiable trust incorporated. The committee recognizes that the Department's

ability to provide superior capabilities to the warfighter is dependent, in part, on its ability to incorporate rapidly evolving, leading-edge microelectronic devices into its defense systems, while also balancing national security concerns. Currently, the Department processes for ensuring trust rely on assessing the integrity of the people and processes used to design, generate, manufacture, and distribute national security critical microelectronics. For over a decade, the Department has relied on a single domestic source for trusted leading edge microelectronics.

However, due to market trends, supply chain globalization, and manufacturing costs, the Department's future access to U.S.-based microelectronics sources is uncertain. As such, the Department is considering various potential approaches that would allow it to access commercial non-trusted sources in the global microelectronics marketplace, while still ensuring trust. Given the Department's reliance on a single source for trusted leading-edge microelectronics, and the dwindling number of domestic microelectronics manufacturers on which the Department can rely, the committee believes that there should be a better understanding of what trust capabilities exist and are in use by the commercial marketplace.

Therefore, the committee directs the Comptroller General of the United States to provide a report to the House Committee on Armed Services by March 30, 2017, that evaluates how selected commercial microelectronics businesses ensure trust. As part of this evaluation, the Comptroller General should address the following:

(1) How do selected commercial companies incorporate trust into their leading-edge microelectronics, including techniques to protect intellectual property and prevent malicious content in devices?

(2) To what extent could the Department of Defense leverage these practices, and what are the challenges associated with implementing these practices for defense systems?

Counter-unmanned aerial systems roadmap

The committee believes that the proliferation of unmanned aerial systems (UAS), particularly small hobby systems that can be bought commercially, pose a significant challenge to the Department of Defense's capabilities to detect, track, and neutralize such threats. The committee is aware that the Army has conducted a technology red team to understand how such systems might be used against U.S. forces, focusing on potential adversarial employment and methods for avoiding detection. The committee is also aware that there has been some preliminary development of counter-UAS capabilities, and that organizations, from the Combating Terrorism Technology Support Office and the Joint Improvised-Threat Defeat Organization, are investigating technology solutions.

However, the committee is increasingly concerned that such efforts are not adequately coordinated, and have focused on near-term capabilities without taking a long-term, integrated view to developing countermeasures. The committee is also

concerned that the current focus does not provide an adequate variety of tools and technologies available at the tactical unit level to detect, track, and neutralize small UAS threats. Therefore, the committee directs the Secretary of Defense to develop a technology roadmap for addressing gaps to counter the potential threats from terrorist or state actor uses of small UAS technology, with an emphasis on technology to support tactical level units, and fixed, high-value defense assets. The committee further directs the Secretary to provide a briefing to the House Committee on Armed Services by June 1, 2017, on this roadmap.

Department of Defense medical countermeasures Advanced Development and Manufacturing facility roadmap

The committee understands the importance of maintaining a broad portfolio of medical countermeasures, including therapeutic and pre-treatment efforts, to address high priority threats to the warfighter. The committee also understands the challenges faced by the Department of Defense medical countermeasure development due to the low quantities procured and other acquisition challenges. The committee is aware of and has been monitoring the Department of Defense Advanced Development and Manufacturing (ADM) capability, which includes a dedicated facility to support the development, licensure, and manufacturing of medical countermeasures. This facility is planned to achieve full operational capability by the end of fiscal year 2016. The committee is also aware of complementary capabilities provided by the Department of Health and Human Services Biomedical Advanced Research and Development Authority (BARDA) Centers for Innovation in Advanced Development and Manufacturing.

The National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92) required the Secretary of Defense to submit a report on the Department of Defense ADM that included cost-benefit analysis of the manufacturing and construction of the facility. The committee continues to be concerned about the potential for long-term operations and maintenance sustainment costs of the Department of Defense ADM facility, and about the possibility for duplication of efforts between the Department of Defense ADM facility and the Department of Health and Human Services ADM facilities. The committee directs the Secretary of Defense to develop and submit a report to the congressional defense committees by December 1, 2016, on the sustainment of the Department of Defense ADM facility. The report should include an estimate of sustainment costs and a roadmap for planned work at the Department of Defense ADM facility over the next 10 years, as well as details on the planned business model for ensuring continued sustainment of the facility. The roadmap should also address partnerships and use of complementary capabilities between the Department of Defense ADM and the Department of Health and Human Services BARDA Centers for Innovation in Advanced Development and Manufacturing.

Desalination technology

The committee is aware the Department of Defense has made advances in desalination technology over the last 15 years in support of large numbers of deployed forces in the Middle East. The committee recognizes that the inability to access clean water is a factor in destabilization around the world. The committee believes sharing desalination technologies with appropriate agencies, like the Department of State, to ensure advances are leveraged in development efforts is an important tool for stability and conflict avoidance. Therefore, the committee directs the Assistant Secretary of Defense for Research and Engineering to provide a briefing to the House Committee on Armed Services not later than March 1, 2017, on recent advances in desalination technologies, and how those advances have been shared with other U.S. Government agencies.

Human systems integration activities

The committee is concerned that military service personnel are required to use systems that are inadequate to their physical, behavioral, and cognitive needs. The committee recognizes that senior service leadership encourages the use of human systems integration research and development methods in response to the National Defense Authorization Act for Fiscal Year 2008 (Public Law 110-181). Despite this, human performance research is not routinely transitioning to defense acquisition programs. Also, with no specifications required for human systems integration in acquisition programs, Requests for Proposals seldom include evaluation criteria for it, and it is ignored by program managers. Nevertheless, the committee notes that individual and team performance is the foundation of an effective military force. Ensuring that systems account for human performance abilities can make acquisitions more cost-effective, strengthen force protection, reduce potential for re-engineering, and cut time and costs of training and re-training, among many other benefits. Therefore, the committee directs the Under Secretary of Defense for Acquisition, Technology, and Logistics to examine Department of Defense policies related to human systems integration within defense acquisitions and to provide a briefing to the House Armed Services Committee by February 15, 2017, on the findings and recommendations necessary to improve inclusion of human system integration research in acquisition programs.

Incentives for increasing private sector medical countermeasures development

The committee is aware of the importance of medical countermeasures, including prophylactics, pre-treatments, diagnostics, and therapeutics, to protect the warfighter from chemical, biological, radiological, and nuclear threats. The committee is also aware of the difficulty in engaging industry partners to develop medical countermeasures due to the low profitability, lengthy process, and costs for doing this contract work for the Government. The committee recognizes that strategies and incentives should be developed to stimulate private sector medical

countermeasures development. Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by February 1, 2017, on potential incentives that would improve private sector, academia, non-profit, and other organization participation in medical countermeasures development. The briefing should identify any incentives that would require additional congressional authorities.

MQ-9 anti-icing capability

The committee notes that an anti-icing capability for the MQ-9 unmanned aerial system has been pursued by the Department of Defense, and specifically U.S. Air Force Air Combat Command, U.S. Special Operations Command, and U.S. Air Force Special Operations Command (AFSOC). However, the committee is concerned that a lack of capability prioritization and technical issues have delayed initial fielding times.

The committee notes that a recent Laboratory Innovation Crowdsourcing (LINC) requirement solicited by the Department's Combating Terrorism Technology Support Office (CTTSO) stated that, "The current MQ-9 was fielded without the exact understanding of how it was affected by icing." The report continued that, "Due to the lack of data, the Air Force imposed conservative flight restrictions in order to reduce the risk to the weapons system ... AFSOC is interested in the development and testing of innovative de-ice technologies that allow the MQ-9 to cruise in light icing and visible moisture." This LINC initiative solicited by CTTSO for outside approaches reinforces the committee's belief that the Department's current approach to satisfying this operational requirement is disjointed and uncoordinated.

Therefore, the committee directs the Secretary of Defense, in coordination with the Commander, U.S. Air Force Air Combat Command and the Commander, U.S. Special Operations Command, to brief the Committee on Armed Services of the U.S. House of Representatives not later than October 1, 2016, on the Department's efforts to field an anti-icing capability for the MQ-9. This briefing shall be in classified form as required.

Prioritization of joint test activities

The committee recognizes that developmental and operational test and evaluation activities are critical steps in research and development programs. Joint programs can be especially complex, and thus substantially more difficult to manage, with competing demands for resources, personnel, service priority, and the need to coordinate over multiple bureaucracies. The committee is concerned that the Department of Defense does not adequately prioritize research and development projects; unfortunately, there are instances when expensive projects from one military department may receive a low priority for testing time and resources at facilities operated by different military departments.

Therefore, the committee directs the Director of the Test Resource Management Center to provide a briefing to the House Committee on Armed Services by December 1, 2016, on the policies and processes for coordinating test and evaluation resources for joint and multi-service research and development projects. The briefing should include recommendations for improving the Department's ability to make cross-service prioritization decisions related to test and evaluation facilities for joint and multi-service programs.

Technology enablers for directed energy weapon systems

The committee is aware that the Department of Defense has made significant advances in the development and operational demonstration of directed energy weapons systems. Each military department has demonstrated a marquee program in this area, such as the Navy's Laser Weapon System deployed on the USS Ponce, the Army High Energy Laser Mobile Demonstrator, and the Marine Corps' Ground Based Air Defense System. Along with technology demonstration activities like the Robust Electric Laser Initiative and the High Energy Liquid Laser Area Defense System, each of these programs demonstrated the increased power output and power on target necessary to develop a militarily useful directed energy weapon.

However, as the Department has made progress in raising the power levels of these systems, it has also demonstrated the need for emphasis on development in other technology areas necessary to realize the full potential of laser weapons. For example, higher power output requires improved beam control to engage targets at greater distances, as well as better thermal management systems to dissipate the increased heat load. As the Department has been overcoming foundational technical challenges, new challenges have emerged that will impact the operational uses for directed energy weapons.

Therefore, the committee directs the Assistant Secretary of Defense for Research and Engineering, in coordination with the research components of the military departments and the High Energy Laser Joint Technology Office, to provide a briefing to the House Committee on Armed Services by January 20, 2017. This briefing should provide a roadmap for enabling technologies, including:

- (1) Beam directors and adaptive optics, including deformable mirrors;
- (2) Thermal management needs and capabilities;
- (3) Integration challenges with fire control systems, including potential future needs for fire control for laser systems;
- (4) Power architectures and power electronics needs;
- (5) Facilities and test range capabilities; and
- (6) Other areas as deemed by the Secretary.

U.S. Special Operations Command rapid prototyping and SOFWERX initiative

The committee notes that the SOFWERX initiative and facility within U.S. Special Operations Command (USSOCOM) creates a forum for accelerating the

delivery of innovative capabilities to U.S. Special Operations Forces (USSOF) by engaging industry, academia, and Government laboratories, as well as hosting innovation and rapid prototyping sessions designed to overcome seemingly intractable problems. The committee notes that these sessions have started to refine and inform current and future USSOF requirements, as well as acquisition and engineering decisions, while increasing the potential to field capabilities faster. The committee applauds this revolutionary approach, which was established by USSOCOM in September 2015 using a Partnership Intermediary Agreement, as defined within section 3715 of title 10, United States Code.

The committee understands that each project within the SOFWERX facility is funded via related research, development, test, and evaluation (RDT&E) programs, including \$0.5 million funded by the Tactical Assault Light Operator Suit effort, and an additional \$2.0 million for fiscal year 2016 within PE 1160402BB, Advanced Technology Demonstrations. For fiscal year 2017, the committee notes that USSOCOM expects to spend \$2.5 million from the Operations and Maintenance, Defense-Wide account for SOFWERX facility and support, although RDT&E efforts are not defined. While these initial investments for SOFWERX appear to be low-dollar thresholds, the committee encourages USSOCOM to seek cost-sharing agreements and cost-saving measures with other Department of Defense entities, such as those within each military service, the Defense Advanced Research Projects Agency, or other non-traditional funding sources when appropriate. The committee encourages USSOCOM to limit growth and overhead of this initiative to ensure affordability across the Future Years Defense Program, and expects to be kept fully and currently informed of the many initiatives expected to spiral from SOFWERX. The committee also expects to be informed of how USSOCOM is sharing technological advances and lessons learned about incentivizing innovation across the Department. Therefore, the committee directs the Commander, U.S. Special Operations Command to provide a briefing to the House Committee on Armed Services by September 1, 2016, on SOFWERX and associated RDT&E efforts.

OPERATIONAL TEST AND EVALUATION, DEFENSE

Items of Special Interest

Range capabilities for emerging advanced technologies

The committee recognizes that the Major Range and Test Facility Base (MRTFB) is a critical component to military technological superiority, and key to ensuring U.S. warfighting capability. This designated core set of Department of Defense Test and Evaluation (T&E) infrastructure, and its associated workforce, is a critical capability to be preserved in order to conduct necessary T&E analyses to support the Department's acquisition process. The committee recognizes that the MRTFB must remain sized, operated, and maintained to preserve core,

governmental T&E capabilities, but should also be developed over time to meet future technology needs of the Department.

The committee is concerned that due to the increased need for protected airspace, as well as increasingly outmoded range technology, many test facilities are difficult to maintain. For example, the open-air test ranges of the MRTFB are not capable of supporting the full spectrum of development testing required for fifth and sixth generation weapon systems, including testing of hypersonic systems, which have been identified as critically important to the third offset strategy. These systems require significant increases in size of contiguous airspace availability, test tracking and data acquisition capabilities, and threat capabilities that exceed current ranges capabilities.

Across the military services, the gaps in range capabilities to meet evolving requirements are growing rapidly. The military services are under pressure to manage modernization of range capabilities to budgets that do not always account for changing technology needs to meet future requirements. Additionally, it is anticipated that the need for increased use of the MRTFB's ranges with large airspace footprints will continue to increase, to support realistic training environments critical to readiness of operational forces. This presents the ranges with growing scheduling capacity challenges, pitting priorities for operational readiness of today's forces against priorities of fielding new system capabilities required to sustain air dominance into the future.

Therefore, the committee directs the Director of the Test Resource Management Center (TRMC) to provide a briefing to the House Committee on Armed Services by March 1, 2017, on the results of a comprehensive assessment of MRTFB needs and investments to meet testing required for fifth and sixth generation aircraft and air armament, including hypersonic strike weapons. This assessment should include the projected requirements of operational forces and other users dependent upon these ranges. The briefing should also include the estimated costs to implement capabilities required to support current and projected future operations, and a plan for ensuring sufficient capacity through a MRTFB range investment plan. Additionally, the committee encourages the TRMC to use the results of this assessment to inform future budget certifications from the military departments and Department of Defense agencies.

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

ITEMS OF SPECIAL INTEREST

Human Capital Plan for Business Transformation

The committee believes that business transformation will be increasingly important to the Department of Defense, especially as shrinking budgets and workforce reductions continue. Additional demands, like the growing

implementation of enterprise resource planning systems for financial and personnel management, as well as the deadlines to reach full financial auditability, further highlight the need to focus on business transformation, and to have a workforce with the right skill sets and experience to ensure that business transformation is successful. As the lead within the Department of Defense for these activities, these workforce needs are especially acute for the Deputy Chief Management Officer (DCMO).

The Government Accountability Office (GAO) has pointed out that the human capital needs for the Office of the DCMO are not completely defined, and that there appear to be gaps in the skill sets needed for that office to be effective. An earlier call to complete a gap analysis of the human capital needs to better understand what types of personnel are needed to manage and oversee business transformation efforts has not been completed. While there is expertise in business systems and process improvement, GAO found the Office of the DCMO lacking in people with strategic planning or performance management expertise. Continuing workforce reductions will not only impact the ability to conduct this sort of assessment, but also underline the needs to take a more focused look at the workforce in order to make strategic decisions about the limited number of people that office will be able to hire and retain.

Therefore, the committee directs the Department of Defense Deputy Chief Management Officer to complete a gap analysis of the human capital needs of the Office of the DCMO, taking into account the merger of the positions of Chief Information Officer and DCMO as directed by section 901 of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113-291), and to provide a briefing to the House Committee on Armed Services by March 1, 2017, on the results of the analysis.

TITLE X—GENERAL PROVISIONS

ITEMS OF SPECIAL INTEREST

OTHER MATTERS

Comptroller General Assessment of Deployable Identity Management Forensics Capability

The committee notes that the Department of Defense has used biometrics and forensics to successfully identify, target, and disrupt terrorists and enemy combatants in the Republic of Iraq and the Islamic Republic of Afghanistan. Expeditionary forensic laboratories have deployed in theater to quickly exploit evidence collected from the battlefield, resulting in the capture and prosecution of enemy combatants. Many of the Department's expeditionary biometrics and forensics capabilities were resourced through the Department's Overseas Contingency Operations funding. The committee notes that the Department has

taken steps to establish expeditionary biometrics and forensics as enduring capabilities in the base budget; however, these funding levels may not be adequate to sustain current and future validated mission requirements.

Therefore, the committee directs the Comptroller General of the United States to assess the Department's process for determining and validating its future expeditionary biometrics and forensics requirements, as well as actions the Department has taken to ensure that its expeditionary biometrics and forensics capabilities, including materiel solutions, trained personnel, and funding, are available to meet current and future requirements. The committee further directs the Comptroller General to provide a briefing to the House Armed Services Committee by March 1, 2017, on the Comptroller General's preliminary findings with a report to follow on a date agreed to at the time of the briefing.

Department of Defense Strategy for Countering Unconventional Warfare

Section 1097 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92) directed the Department of Defense to develop a strategy to counter unconventional warfare threats posed by adversarial state and non-state actors. Section 1097 further directed the Secretary of Defense and the Chairman of the Joint Chiefs of Staff to coordinate this strategy with the heads of other appropriate departments and agencies of the U.S. Government. The Secretary is required to submit this strategy to the congressional defense committees not later than 180 days after the date of the enactment of Public Law 114-92.

The committee remains concerned about the growing unconventional warfare capabilities and threats being posed most notably and recently by the Russian Federation and the Islamic Republic of Iran. The committee notes that unconventional warfare is defined most accurately as those activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, or guerrilla force in a denied area. The committee also notes that most state-sponsors of unconventional warfare, such as Russia and Iran, have doctrinally linked conventional warfare, economic warfare, cyber warfare, information operations, intelligence operations, and other activities seamlessly in an effort to undermine U.S. national security objectives and the objectives of U.S. allies alike.

The committee also notes that the Department of Defense may require additional time to fully and properly coordinate the strategy, as directed by section 1097, with the heads of other appropriate departments and agencies of the U.S. Government. Given the importance of this coordination and the interagency aspects of an effective strategy for countering unconventional warfare threats, the committee expects frequent and periodic progress updates by the Department should an extension be required for interagency coordination and the development and delivery of this strategy. Therefore, the committee directs the Secretary of Defense to provide an update to the Committees on Armed Services of the Senate and the House of Representatives by May 23, 2016, on the completion of the

strategy for countering unconventional warfare threats required by section 1097 of Public Law 114-92.

Wassenaar Arrangement Impacts to the Department of Defense

The committee understands the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies prevents destabilizing accumulations of covered goods and technologies, and seeks to prevent acquisition of such items by terrorists. Covered technologies and goods subject to the Wassenaar Arrangement impact items which have both military and civilian applications. For example, controls for software, hardware, and technology that operate, deliver, or communicate with intrusion software added to the list of dual-use technologies in 2013 include a number of products regularly used for cyber security research and defense. The committee believes restricting export of these technologies may negatively impact use of such products for national security purposes. Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by March 1, 2017, on the impact of the Wassenaar Agreement to Department of Defense applications, including efforts to support alliance partners or otherwise build partner capacity with friendly nations.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

ITEMS OF SPECIAL INTEREST

Countering Adversarial Messaging

The committee remains concerned about the success of the Islamic State of Iraq and the Levant (ISIL) messaging and propaganda, and their ability to persuade, inspire, and recruit from across the globe. ISIL's continued success on the battlefield depends on this messaging, and the group's propaganda attracts recruits and other support that enables it to persist. Consequently, the committee believes that the campaign to degrade and defeat ISIL on the battlefield must be linked with a comparable effort to degrade and defeat ISIL's message in the minds of potential supporters. The committee recognizes that other extremist groups have taken note of ISIL's success and are expanding their messaging operations, particularly in social media.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by March 17, 2017, on the Department of Defense's long-term strategy to counter adversarial messaging and recruiting utilizing digital technologies, including social media. The briefing should address the following questions:

- (1) What are the Department's roles, responsibilities, and rules of engagement when it comes to countering adversarial messaging?

- (2) What is the Department's integrated strategy to counter online radicalization and recruitment?
- (3) What measures of effectiveness exist to inform outcomes?
- (4) What analytical data points have already been collected to compare our capabilities to those of our adversaries?
- (5) What policies, regulations, or other guidance need to be updated or modified to improve the Department's ability to execute an integrated strategy?

Reporting Requirements of Authority for Support of Special Operations to Combat Terrorism

The committee notes the importance of the Authority for Support of Special Operations to Combat Terrorism, as provided in section 1208 of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Public Law 108-375), as most recently amended by section 1274 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92). The committee directs the Secretary of Defense to notify the congressional defense committees of funding changes to programs executed under this authority when such a proposed increase exceeds 20 percent of the currently approved total for that particular program, or \$1.0 million; whichever amount is less.

Social Media Analytics and Publically Available Information Supporting Battlespace Awareness

The committee remains concerned with the Department of Defense's ability to effectively monitor and utilize social media analytic tools to support awareness of the operating environment for force protection, operational security, and other missions. The committee believes that the lack of clearly defined policies is hampering the ability to use such Publicly Available Information (PAI) to understand adversarial sentiment and narrative messaging in theaters of active hostilities, as well as monitoring for non- and semi-permissive environments, and areas of potential future activity. While there are some technology capabilities that currently exist that could support these activities, including many that can be leveraged from the commercial sector, the committee believes that the Department of Defense is not effectively leveraging these tools because of a fundamental lack of policy, doctrine, and procedures that delineate how such tools might be used. In the lack of such guidance, the committee believes that the Department is abdicating this space to adversaries that have no compunction to limit their actions, and in fact actively exploit it to achieve their strategic goals of recruitment, fundraising, and strategic messaging.

The committee notes that PAI use and exploitation is having a revolutionary impact on both operations and intelligence within the Department. Further, the committee recognizes that while intelligence activities have important uses for PAI, the Department also has unique operational uses and requirements for PAI that support force protection, targeting, battlespace awareness, and other

traditional military activities. As a result, the demand signal for the operational use of PAI has increased across the force.

Therefore, the committee directs the Secretary of Defense to conduct an assessment of the current policy directives on how defense entities use such social media tools, and to provide a briefing on this assessment to the House Committee on Armed Services by February 15, 2017. This assessment should examine the demand for such capabilities from the combatant commanders to identify any gaps or areas needing clarification in policy, doctrine, training, and technology capabilities. In conducting this assessment, the Secretary should consider operational missions for social media analytics, such as battlespace awareness, operational security, and sentiment analysis for counter-messaging adversarial narratives and the operational use of PAI. The assessment should also include a discussion of legal and policy issues associated with the use of PAI, as well as resource limitations, approval processes, training requirements, and steps being taken to improve coordination of effort and leverage best practices and capabilities across the Department. Finally, the Secretary should report on how to continue and enhance capabilities to ensure U.S. persons' PAI is not inadvertently viewed, as well as methods for addressing inadvertent viewing while in enemy battlespace.

Strategy for Regional Counter-Narrative Capabilities

The committee remains concerned with the success of Islamic State of Iraq and the Levant's (ISIL) messaging and propaganda, and ISIL's ability to persuade, inspire, and recruit from across the globe. ISIL's continued success on the battlefield depends on this messaging, and the group's propaganda attracts recruits and other support that enables the organization to persist. Consequently, the committee believes that the campaign to degrade and defeat ISIL on the battlefield must be matched with a comparable effort to degrade and defeat ISIL's message in the minds of potential supporters.

The committee is also aware that Russian actors have been highly effective in shaping the information environment against Ukrainian forces, as well as against other actors in the region seeking to counter Russian influence. The ambiguity that these information operations create has been critical in the hybrid and unconventional warfare strategy of Russian forces, and have effectively masked, created confusion, or otherwise undermined timely reactions from Western and allied forces.

Not only does the Department need to consider how adversaries use such information strategies to support their operations and undermine our own, but the committee believes that the Department should be developing an integrated strategy that can leverage, and when necessary combine with, allied and partner capabilities to maximize our messaging and its broader effects. The committee also believes that there are useful technologies, training, and strategies that U.S. forces could use to support allied, and international, partner information operations

capabilities to mitigate and marginalize adversaries' ability to influence and inspire.

Therefore, the committee directs the Secretary of Defense to develop and submit a strategy for regionally building partnership capacity to the House Committee on Armed Services by June 1, 2017. This strategy should look at means for monitoring, data collection of narratives, and development of networks for countering narratives to support the missions of the combatant commands. Additionally, this strategy should outline how to leverage existing partnership funds to support regional cooperation, as well as prioritize the types of capacity building that could take place, and the regional partners that are most mature to conduct this kind of capacity building.

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

ITEMS OF SPECIAL INTEREST

Assessment of Department of Defense Efforts to Secure Internet of Things

The proliferation of embedded computing systems within the Department of Defense has provided significant capabilities that have enabled battlefield superiority, created realistic training environments, facilitated the tracking of supplies and equipment, improved health care provided to wounded soldiers, and provided common operating pictures to support command and control decisions. However, as these and future capabilities become more connected to the Internet, the success, security, and resilience of the Department's missions, personnel, and capabilities could become jeopardized. For example, the same systems that allow commanders to provide command and control or have situational awareness of troop movement from remote locations could be used by enemies or other bad actors to identify, track, and even misdirect U.S. and allied forces. Further, while the Department tries to mitigate Internet-based threats that could emanate from or use Department of Defense networks, the Department may remain vulnerable based on the reliance on non-defense networks, such as those from defense industrial base partners or allies. Those systems may collect and store critical information the Department is reliant on, and thus weaknesses in the security of those systems may have inadvertent impacts on Department of Defense data and networks.

Therefore, the committee directs the Comptroller General of the United States to assess the Department of Defense's planning and management for the security impact and challenges that the Internet of Things will present to the Department. The committee directs the Comptroller General to provide a report on the findings to the Committees on Armed Services of the Senate and the House of Representatives. The Comptroller General should provide a briefing on preliminary results to the House Committee on Armed Services by March 1, 2017, with the

report to follow on a date agreed to at the time of the briefing. The assessment should address the following:

(1) To what extent does the Department have situational awareness of the extent to which its current capabilities are exposed to Internet-based threats and the vulnerabilities that could result; and what actions, if any, is the Department taking to mitigate these threats?

(2) To what extent does the Department have policies and plans in place to monitor, track, report, and manage incidents where the Department's Internet-based capabilities are accessed or manipulated?

(3) To what extent has the Department taken action to manage the security of Internet-based capabilities being procured by Department of Defense components?

(4) Any other matters the Comptroller General determines are relevant.

Cloud Access Points

The committee remains supportive of enabling the adoption of cloud computing throughout the Department of Defense in order to realize cost savings and efficiency, as well as increased agility and security. The committee recognizes that the Department must develop the necessary security requirements to ensure that sensitive missions and data are protected from evolving cyber threats. However, the committee is concerned that the current Department approach to protecting the Department of Defense Information Network from outside intrusions through the Cloud Access Point (CAP), for data classified as Information Impact Level 4 and above, may impede the adoption of cloud-based commercial solutions due to inadequate implementation of the CAP to date. This approach may also impede the limitations the current CAP model places on the Department's ability to scale with commercial cloud service providers.

In order to move forward with the adoption of cloud computing, the committee believes the Department should implement the current CAP iteration to allow the movement of eligible data to the Federal Risk and Authorization Management Program accredited commercial cloud providers in the short-term. The Department should also consider developing a strategy for the development and implementation of a more capable CAP program that enables greater adoption of commercial cloud, while also evolving with cybersecurity threats.

Therefore, the committee directs the Department of Defense Chief Information Officer to provide a briefing to the House Committee on Armed Services, not later than December 1, 2016, with an update on the status of the implementation of the current CAP program. The briefing should include the identification of near-term steps necessary to implement the current CAP program goals and objectives, in addition to long-term goals and requirements to evolve and improve the CAP program. Finally, the briefing should also include emerging standards and practices to address intrusion detection and institute appropriate firewalls on any defense network utilizing the CAP program.

Comptroller General Assessment of the Management and Measurement of Cyber Activities

The committee notes that the Department of Defense's primary cybersecurity mission is to defend its own networks, systems, and information, and if the Department's systems are not dependable in the face of cyber warfare, all other missions are at risk. The committee is aware that a cyber incident could have significant impact on the Department, including loss of confidence in national security, loss of national security or personal identifiable information, and the inability to conduct military operations.

The committee recognizes that it is imperative that Department leaders, commanders, and supervisors at all levels implement cybersecurity discipline, enforce accountability, manage the shared risk to all Department missions, and take action as soon as possible, because a weakness in one part of the Department's network is a vulnerability and potential back door to other parts of the network. Recently, senior Department leaders have issued important cybersecurity guidance to help manage and focus cybersecurity efforts. Among these are a revised Department Cyber Strategy, a Cybersecurity Campaign memo, cybersecurity execute orders, a Department Cybersecurity Scorecard, and Cybersecurity Discipline Implementation Plan.

The committee also recognizes that it has been 6 years since U.S. Cyber Command became fully operational, and that the effectiveness of the dual-hat relationship between the director of the National Security Agency and the commander of United States Cyber Command has been a matter of concern. The committee believes that the right balance of effective management, tone established at the top, and Department-wide commitment to defense cybersecurity matters is vital to ensuring success in the Department's cyber efforts. Prior assessments by the Government Accountability Office (GAO) have highlighted management weaknesses across the Department, and made recommendations that could improve the Department's cybersecurity posture.

Therefore, the committee directs the Comptroller General of the United States to assess the Department of Defense's management and measurement of progress in protecting its own networks, systems, and information, and to provide a report on the findings to the Committees on Armed Services of the Senate and the House of Representatives by April 15, 2017. The assessment should address the following:

- (1) What are the benefits and drawbacks of maintaining a dual-hat relationship between the director of the National Security Agency and the commander of U.S. Cyber Command, and how is the Defense Department measuring the performance of this relationship?
- (2) To what extent has the Department made progress in implementing key cybersecurity guidance, such as the Defense Cyber Strategy, the Cybersecurity Campaign, and the Cybersecurity Scorecard?

(3) To what extent has the Department implemented recommendations from GAO assessments of the Department's management of cybersecurity issues?

(4) Any other matters the Comptroller General determines are relevant.

The committee further directs the Comptroller General to provide a briefing to the House Committee on Armed Services by March 1, 2017, on the Comptroller General's preliminary findings.

Cyber Training Equivalency

The committee is aware that the Department of Defense is in the process of rapidly expanding the cyber workforce in order to man the 133 teams of the cyber mission force. As articulated by the Commander of U.S. Cyber Command, the committee recognizes that a significant bottleneck in that process is the training pipeline. The committee believes that the Department should be looking for opportunities to help diversify the training pathways available to all members of the cyber mission team workforce, in order to more quickly and efficiently bring team members up to operational capacity. The committee believes that diversification can take many forms, such as utilization of Reserve Officer Training Corps courses, military academies, public-private partnerships with universities and other training providers, and senior leader military academies. The committee also believes that to make those other training pathways effective, the Department needs to have a robust process for determining equivalency, so that it is clear when those other avenues can be used to meet the currently defined joint training standard. The committee is concerned that the immaturity of that equivalency process may be further slowing up the training pipeline.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by January 30, 2017, on the training equivalency process for the Department. This briefing should address how the Department makes recommendations on equivalency for members of the active and reserve components, as well as for civilian team members. Specifically, this briefing should include:

(1) What is the decision making chain for making equivalency decisions?

(2) How does the Department communicate standardized courses that are eligible for equivalency?

(3) When equivalency is denied, what is the feedback loop to communicate those decisions back to affected personnel?

(4) What is the process for remediation for service members to determine what actions might be taken to gain equivalency certification?

Host Based Security System Best Practices

The committee is aware that the Host Based Security System (HBSS) has become an increasingly effective tool to manage the cyber defense of the Department of Defense. HBSS is a capability that monitors, detects, and counters

known cyber threats to the Department, and includes commercially available intrusion detection and firewall capabilities.

The committee notes that in recent cyber exercises conducted by United States Cyber Command, HBSS has been the primary warfighting system for cyber defenders. However, the committee is also aware from after action reviews and discussions with senior leaders from the military departments and Cyber Command, that the results from the various teams are uneven, in terms of how well they employ HBSS in these exercises. While some variation in learning and execution can be useful, the committee believes that the military services should be learning and implementing best practices to improve how HBSS is used.

Therefore, the committee directs the Department of Defense Chief Information Officer, in coordination the military departments and the Defense Information Systems Agency, to provide a briefing to the House Committee on Armed Services by August 1, 2017, on the best practices and lessons learned for use and configuration for the Host Based Security System. This briefing should include:

- (1) Recommendations for configurations or implementations that have proven successful in recent training exercises where HBSS is used, as well as from real-world operational experiences with HBSS;
- (2) Identification of opportunities to better leverage capabilities inherent in the current technology solution, such as digital rights management, including scenario development for how such tools might be used in future exercises; and
- (3) Identification of gaps from the operational community that might be found in other commercially available tools that could potentially be integrated into future generations of HBSS or follow-on programs.

Information Assurance of Joint Test and Evaluation Activities

The committee recognizes that information assurance policies continue to be disjointed, often redundant, and overly complex and cumbersome. That problem is highlighted by how those challenges manifest in the joint test and evaluation (T&E) community. As noted elsewhere in this report, joint programs can be especially complex, and thus substantially more difficult to manage. When network information assurance policies from the various military departments are included in that mix, it often results in unnecessary program delays and bureaucratic red tape. The lack of clear guidance or reciprocity for information assurance policies is a significant factor in this problem.

Therefore, the committee directs the Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the Department of Defense Chief Management Officer, to provide a briefing to the House Committee on Armed Services by January 13, 2017, assessing the policies and processes for coordinating information assurance policies on test and evaluation facilities when conducting joint or multiservice T&E activities. The briefing should also make recommendations for improving reciprocity or prioritization of interagency policies related to T&E facilities when conducting joint or multiservice activities.

Insider Threat Capabilities for the Joint Information Environment

The committee is aware that the Department of Defense is continuing to implement an initiative known as the Joint Information Environment (JIE) that is intended to streamline, standardize, and modernize the information network of the Department and the military services. A key part of the strategy to implement JIE is development of a single security architecture that will improve network monitoring and defense of the JIE.

The committee notes that the primary focus of network monitoring and defense has been on external threats to the network. However, the committee is concerned about the threat from insiders, as well as the ability for adversaries to move laterally within a network once they have penetrated barrier defenses. Historically, the tools used to monitor those exterior threats do not provide good defenses against insiders or lateral movements within a network. Where the Department has been focused on insider threats, the committee is concerned that those recommendations have been focused on procedural changes that are not connected to the capabilities, or the capability needs, for network tools and digital rights management.

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 December 1, 2016, on how insider threat capabilities are planned to be integrated into the JIE. This briefing should address those tools currently planned for incorporation, like digital rights management, as well as identification of any gaps in the architecture where commercial tools for insider threat monitoring might be included into JIE, or into upgrades to key enabling capabilities like the Joint Regional Security Stacks or the Host Based Security System.

Strategic Plan for the Defense Insider Threat Management and Analysis Center

The committee is aware that the Department of Defense established the Defense Insider Threat Management Analysis Center (DITMAC) in order to consolidate and analyze specified defense reporting of potentially adverse information, to include potential insider threat information. Specifically, the DITMAC has the following missions:

(1) Oversee the mitigation of insider threats to defense personnel, infrastructure, and essential national security information resident on defense facilities or networks;

(2) Develop risk thresholds and standards for actions, and compile results to evaluate those actions on threats that insiders may pose to their colleagues, defense missions, and resources;

(3) Establish standards to ensure the Department's Insider Threat Program is compliant with applicable executive orders and regulations;

(4) Fulfill certain requirements of national insider threat policy and minimum standards; and

(5) Promote collaboration and information sharing on insider threats to defense personnel and facilities.

While the DITMAC is a relatively new capability that is still scaling up to conduct its defined missions, the need for a robust insider threat capability is important and will continue to grow in the future. Additionally, with the Department's new responsibilities for developing and sustaining the information technology resources related to personnel security clearances, the DITMAC has the potential to support that mission area as well.

Therefore, the committee directs the Director of the Defense Security Services to develop and submit a strategic plan for the DITMAC to the congressional defense committees and the congressional intelligence committees, not later than June 1, 2017. This strategic plan should address the needed technical capabilities, such as digital rights management, as well as updated policies, and workforce considerations to adequately execute its missions, and a concept of operations for how the DITMAC might scale if needed to support the personnel security clearance analysis needs of the Department.